

p. 75

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-359616

(43)Date of publication of application : 13.12.2002

(51)Int.Cl. H04L 9/08
G09C 5/00
H04L 9/00
H04L 9/32

(21)Application number : 2002-
028915

(71)Applicant : SONY CORP

(22)Date of filing : 06.02.2002

(72)Inventor : TANAKA KOICHI
KAWAKAMI TATSU
KURODA HISASUKE
ISHIGURO RYUJI

(30)Priority

Priority number : 2001033114 Priority date : 09.02.2001 Priority country : JP
2001094803 29.03.2001 JP

(54) INFORMATION PROCESSOR AND METHODLICENSE SERVERAND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To freely distribute contents and allow only authorized users to utilize the contents.

SOLUTION: A client receives an encrypted content from a content server. The header of the content includes license-identifying information for identifying a license required in utilization of the content. The client requests a license server to transmit a license identified by the license-identifying information. When receiving the request for a licensethe license server carries out a charging process before transmitting the license to the client. The client can decode and play back the content on the condition of possessing the license.

CLAIMS

[Claim(s)]

[Claim 1]An information processor comprising:

License: specific information for specifying said license which carries out the utilization permission of the contents concerned in an information processor which permits use of contents on condition that a license is held.

Enciphered contents data.

A content storing means which memorizes said contents including key information required in order to decode contents data.

A license memory measure which memorizes a license containing contents specific information for specifying said contents by which a utilization permission is carried outA judging means which judges whether a license which can carry out the utilization permission of said contents is memorized by said license memory measureand a decoding means which decodes contents data of said contents on condition that it was judged that a license was memorized by said judging means.

[Claim 2]The information processor according to claim 1 which is provided with the following and characterized by a license received by said reception means being memorized by said license memory measure.

A transmitting means which transmits a license request containing license identification information for said information processor to identify a license to a license server further.

A reception means which receives a license transmitted by license server.

[Claim 3]The information processor according to claim 1wherein said contents data is further provided with a reproduction means which reproduces contents data which is the data which combined text dataimage datavoice dataa video dataor themand was decoded by said decoding means.

[Claim 4]Said key information contains EKB (Enabling Key Block)Said information processor is provided with a device node key memory measure which memorizes a device node key furtherSaid decoding means said EKB (Enabling Key Block) using a route key by which decoding processing might be carried out using said device node key memorized by said device node key memory measure said enciphered contents data. The decoding information processor according to claim 1.

[Claim 5]Said key information contains a contents key further enciphered by route key of said EKB (Enabling Key Block)Said contents data is enciphered by said contents keySaid decoding means said contents key decoded using a route key by which decoding processing might be carried out in said EKB (Enabling Key Block) using said device node key memorized by said device node key memory measure. The information processor according to claim 4 using and decoding said enciphered contents data.

[Claim 6]The information processor according to claim 1wherein said license includes service-condition information which shows further a service condition of contents which become available according to the license concerned.

[Claim 7]The information processor according to claim 1wherein said license includes further an electronic signature made with a secret key of a license server.

[Claim 8]Said information processor is provided with a terminal-identification-

information memory measure which memorizes terminal identification information which identifies an information processor further Said license request includes further said terminal identification information memorized by terminal-identification-information memory measure Further said license received by said reception means including said terminal identification information said judging means Said terminal identification information included in said license is compared with said terminal identification information memorized by said terminal-identification-information memory measure The information processor according to claim 2 restricting when both are in agreement and judging that the license concerned is a license to which use of said contents is permissible.

[Claim 9] An information processing method with which use of contents is permitted on condition that a license characterized by comprising the following is held.

License specific information for specifying said license which carries out the utilization permission of the contents concerned.

Key information required in order to decode enciphered contents data and contents data.

[Claim 10] A program which makes a computer perform processing to which use of contents is permitted on condition that a license characterized by comprising the following is held.

License specific information for specifying said license which carries out the utilization permission of the contents concerned.

Key information required in order to decode enciphered contents data and contents data.

[Claim 11] The program according to claim 10 wherein said program or its part is enciphered.

[Claim 12] A license server which publishes a license to which use of contents is permitted comprising:

Contents specific information for specifying said contents a utilization permission is carried out by the license concerned of.

A reception means which receives a license request containing license identification information which was transmitted from a license memory measure which memorizes said license including terminal identification information which identifies an information processor and an information processor and which identifies a license.

An extraction means to extract said license corresponding to said license identification information contained in said license request from said license memory measure.

A processing means to add said terminal identification information to said license extracted by said extraction means.

A signature means which adds an electronic signature to a license to which terminal identification information was added by said processing means using a

secret key of a license server.

A transmitting means which transmits a license signed by said signature means to an information processor which transmitted said license request.

[Claim 13]An information processing method which publishes a license to which use of contents is permittedcomprising:

Contents specific information for specifying said contents a utilization permission is carried out by the license concerned of.

A step which memorizes said license including terminal identification information which identifies an information processor.

A step which receives a license request containing license identification information which was transmitted from an information processorand which identifies a license.

A step which extracts said license corresponding to said license identification information contained in said license request from said license memory measureA step which adds said terminal identification information to said license extracted by said extraction meansA step which adds an electronic signature to a license to which terminal identification information was added by said processing means using a secret key of a license serverand a step which transmits a license signed by said signature means to an information processor which transmitted said license request.

[Claim 14]Contents specific information for being a program which makes a computer perform processing processing which publishes a license to which use of contents is permittedand specifying said contents a utilization permission is carried out by the license concerned ofA step which memorizes said license including terminal identification information which identifies an information processorA step which receives a license request containing license identification information which was transmitted from an information processorand which identifies a licenseA step which extracts said license corresponding to said license identification information contained in said license request from said license memory measureA step which adds said terminal identification information to said license extracted by said extraction meansA step which adds an electronic signature to a license to which terminal identification information was added by said processing means using a secret key of a license serverA program which makes a computer perform a step which transmits a license signed by said signature means to an information processor which transmitted said license request.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention about an information processor and a method a license server and a programThe contents which have not been licensed in particular from an owner of a copyright are copied unjustly and are related with the information processor and the method license server and program which enabled it to prevent being used.

[0002]

[Description of the Prior Art]These days as a user provides other users with the music data which he holds via the Internet and offers are received for the music data which he does not hold from other users the system where two or more users exchange music data for nothing and which they suit is realized.

[0003]If the contents of one music and others exist theoretically in order that other users of all the may be enabled to use it and many users may not purchase contents in such a system Since the owner of a copyright about contents cannot sell the contents as works he will lose an opportunity to receive the loyalty about use of the works which can originally be received with sale of works.

[0004]

[Problem(s) to be Solved by the Invention]Then it is requested socially that it should prevent being used unjustly without barring circulation of contents.

[0005]This invention is made in view of such a situation and it enables it to prevent contents from being used unjustly certainly.

[0006]

[Means for Solving the Problem]License specific information for specifying a license required in order that an information processor of this invention may carry out the utilization permission of the contents A content storing means which memorizes contents including enciphered contents data and key information required in order to decode contents data A license memory measure which memorizes a license containing contents specific information for specifying contents by which a utilization permission is carried out A judging means which judges whether a license which can carry out the utilization permission of the contents is memorized by license memory measure It has a decoding means which decodes contents data of contents on condition that it was judged that a license was memorized by a judging means.

[0007]A transmitting means which transmits a license request containing license identification information for an information processor to identify a license to a license server further It has a reception means which receives a license transmitted by license server and a license received by a reception means can be memorized by license memory measure.

[0008]Contents data is the data which combined text data image data voice data a video data or the and can be further provided with a reproduction means which reproduces contents data decoded by decoding means.

[0009]Key information contains EKB (Enabling Key Block) An information processor is provided with a device node key memory measure which memorizes a device node key further The decoding means can decode contents data enciphered using a route key by which decoding processing might be carried out in EKB

(Enabling Key Block) using a device node key memorized by device node key memory measure.

[0010]Key information contains a contents key further enciphered by route key of EKB (Enabling Key Block)Contents data is enciphered by contents keyA decoding means contents data enciphered using a contents key decoded using a route key by which decoding processing might be carried out in EKB (Enabling Key Block) using a device node key memorized by device node key memory measure. It can decode.

[0011]The license can include service-condition information which shows further a service condition of contents which become available according to the license.

[0012]The license can include further an electronic signature made with a secret key of a license server.

[0013]An information processor is provided with a terminal-identification-information memory measure which memorizes terminal identification information which identifies an information processor furtherFurther a license with which a license request was further received by a reception means including terminal identification information memorized by terminal-identification-information memory measure including terminal identification information a judging meansTerminal identification information included in a license is compared with terminal identification information memorized by terminal-identification-information memory measurewhen both are in agreementit restrictsand it can judge that the license is a license to which use of contents is permissible.

[0014]License specific information for an information processing method of this invention to specify a license which carries out the utilization permission of the contentsEnciphered contents data and key information required in order to decode contents dataA step which memorizes a step which memorizes ***** contentsand a license containing contents specific information for specifying contents by which a utilization permission is carried outA step which judges whether a license which can carry out the utilization permission of the contents is memorized by license memory measureA step which decodes contents data of contents on condition that it was judged that a license was memorized by a judging means is included.

[0015]License specific information for a program of this invention to specify a license which carries out the utilization permission of the contentsEnciphered contents data and key information required in order to decode contents dataA step which memorizes a step which memorizes ***** contentsand a license containing contents specific information for specifying contents by which a utilization permission is carried outA step which judges whether a license which can carry out the utilization permission of the contents is memorized by license memory measureA computer is made to perform a step which decodes contents data of contents on condition that it was judged that a license was memorized by a judging means.

[0016]A program or its part can be enciphered.

[0017]Since contents permitted are specifiedthis invention is characterized by a

license server comprising the following.

Contents specific information.

A license memory measure which memorizes a license including terminal identification information which identifies an information processor.

A reception means which receives a license request containing license identification information which was transmitted from an information processor and which identifies a license.

An extraction means to extract a license corresponding to license identification information contained in a license request from a license memory measure.

A processing means to add terminal identification information to a license extracted by an extraction means.

A signature means which adds an electronic signature to a license to which terminal identification information was added by a processing

means using a secret key of a license server.

A transmitting means which transmits a license signed by a signature means to an information processor which transmitted a license request.

[0018] Since contents by which a utilization permission is carried out are specified, this invention is characterized by an information processing method comprising the following.

Contents specific information.

A step which memorizes a license including terminal identification information which identifies an information processor.

A step which receives a license request containing license identification information which was transmitted from an information processor and which identifies a license.

A step which extracts a license corresponding to license identification information contained in a license request from a license memory measure.

A step which adds terminal identification information to a license extracted by an extraction means.

A step which adds an electronic signature to a license to which terminal

identification information was added by a processing means using a secret key of a

license server.

A step which transmits a license signed by a signature means to an information processor which transmitted a license request.

[0019] In an information processor of this invention, an information processing method and a program on condition that a license is held, contents are decoded and it is made available.

[0020] In a license server of this invention, an information processing method and an effective license is published only with a specific information processor.

[0021]

[Embodiment of the Invention] Drawing 1 shows the composition of the contents providing system which applied this invention. Client 1-11-2 (hereafter, when these clients do not need to be distinguished separately, the client 1 is only called) is connected to the Internet 2. In this example, although two clients are shown, the client of the arbitrary number is connected to the Internet 2.

[0022]On the Internet 2. When the contents server 3 which provides contents to the client 1the license server 4 which gives a license required to use the contents which the contents server 3 provides to the client 1and the client 1 receive a licenseThe fee collection server 5 which performs accounting to the client 1 is connected.

[0023]These contents servers 3the license server 4and the fee collection server 5 are also connected to the arbitrary number and the Internet 2.

[0024]Drawing 2 expresses the composition of the client 1.

[0025]In drawing 2CPU(CentralProcessing Unit) 21Various kinds of processings are performed according to the program memorized by ROM(Read Only Memory) 22 or the program loaded to RAM(Random Access Memory) 23 from the storage parts store 28. the timer 20 — a time check — it operates and time information is supplied to CPU21. To RAM23CPU21 performs various kinds of processings againand also required data etc. are memorized suitably.

[0026]The encryption decoding part 24 performs processing which decodes the already enciphered contents data while enciphering contents data. The codec part 25 encodes contents data by ATRAC(Adaptive Transform Acoustic Coding)3 method etc.for exampleIt is made to supply and record on the semiconductor memory 44 connected to the drive 30 via the input/output interface 32. Or the codec part 25 decodes the data which was read from the semiconductor memory 44 via the drive 30 and which is encoded again.

[0027]The semiconductor memory 44 is constituted by the memory stick (trademark) etc.for example.

[0028]CPU21ROM22RAM23the encryption decoding part 24and the codec part 25 are mutually connected via the bus 31. The input/output interface 32 is also connected to this bus 31 again.

[0029]The input part 26CRT which become the input/output interface 32 from a keyboarda mouseetc.The communications department 29 which comprises the storage parts store 28a modema terminal adopteretc. which comprise the outputting part 27 which consists of a display which consists of LCD etc.a loudspeakeretc.a hard disketc. is connected. The communications department 29 performs the communications processing through the Internet 2. The communications department 29 performs the communications processing of an analog signal or a digital signal among other clients again.

[0030]The drive 30 is connected to the input/output interface 32 again if neededIt is suitably equipped with the magnetic disk 41the optical disc 42the magneto-optical disc 43or the semiconductor memory 44and the computer program read from them is installed in the storage parts store 28 if needed.

[0031]Although a graphic display is omittedthe contents server 3the license server 4and the fee collection server 5 are also constituted by the client 1 shown in drawing 2and the computer which has the same composition fundamentally. Thenin the following explanationthe composition of drawing 2 is quoted also as composition of the contents server 3the license server 4the fee collection server 5etc.

[0032]Nextwith reference to the flow chart of drawing 3the client 1 explains the processing which receives offer of contents from the contents server 3.

[0033]When a user orders it access to the contents server 3 by operating the input part 26CPU21 controls the communications department 29 and he makes it access the contents server 3 via the Internet 2 in Step S1. In Step S2a user operates the input part 26and if the contents which receive offer are specifiedCPU21 will receive this specification information and will notify the contents specified as the contents server 3 via the Internet 2 from the communications department 29. The contents server 3 which received this notice so that it may mention later with reference to the flow chart of drawing 4Since the enciphered contents data is transmittedin Step S3 CPU21If this contents data is received via the communications department 29that contents data enciphered will be supplied and stored in the hard disk which constitutes the storage parts store 28 in step S4.

[0034]Nextwith reference to the flow chart of drawing 4contents offer processing of the contents server 3 corresponding to the above processing of the client 1 is explained. In the following explanationthe composition of the client 1 of drawing 2 is quoted also as composition of the contents server 3.

[0035]In Step S21CPU21 of the contents server 3It stands by until it receives access from the Internet 2 from the client 1 via the communications department 29and when it judges with having received accessit progresses to Step S22 and the information which specifies the contents transmitted from the client 1 is incorporated. The information which specifies these contents is information which the client 1 has notified in Step S2 of drawing 3.

[0036]In Step S23CPU21 of the contents server 3 reads the contents specified for the information incorporated by processing of Step S22 out of the contents data memorized by the storage parts store 28. CPU21 supplies the contents data read from the storage parts store 28 to the encryption decoding part 24and makes it encipher in Step S24 using the contents key Kc.

[0037]Since the contents data memorized by the storage parts store 28 is already encoded by the codec part 25 with ATRAC3 methodthis contents data encoded will be enciphered.

[0038]Of coursethe storage parts store 28 can be made to memorize contents data in the state where it enciphered beforehand. In this caseprocessing of Step S24 can be omitted.

[0039]Nextin Step S25 CPU21 of the contents server 3Key information (EKB and K_{EKB} (Kc) which are later mentioned with reference to drawing 5) required to decode the contents enciphered by the header which constitutes the format which transmits the enciphered contents dataLicense ID for identifying a license required to use contents is added. And in Step S26 CPU21 of the contents server 3The data which formatted the key and the header which added license ID is transmitted to the accessed client 1 via the Internet 2 from the communications department 29 at the contents enciphered by processing of Step S24and processing of Step S25.

[0040] Drawing 5 is carried out in this way and expresses the composition of the format in case contents are supplied to the client 1 from the contents server 3. This format is constituted by header (Header) and the data (Data) as shown in the figure.

[0041] In a header contents information (Content information) Digital-rights-management information (DRM (Digital Right Management) information) license ID (License ID) and an INEBU ring key block (validation key blocks) (EKB (Enabling Key Block)) — and Data K_{EKBC} (K_c) as the contents key K_c enciphered using key K_{EKBC} generated from EKB is arranged. EKB is later mentioned with reference to drawing 15.

[0042] Information including the method etc. of the content ID (CID) as identification information for identifying the contents data by which formatting is carried out as data and the codec of the contents is included in contents information.

[0043] The rule and state (User rules/status) which use contents for digital-rights-management information and URL (Uniform Resource Locator) are arranged. The reproduction frequency of contents copy frequency etc. are described by a use rule and the state for example.

[0044] URL is address information accessed when acquiring the license specified by license ID and is an address of the license server 4 specifically required in the case of the system of drawing 1 since it is licensed. License ID identifies the license needed when using the contents currently recorded as data.

[0045] Data is constituted by arbitrary numbers of encryption blocks (Encryption Block). Each encryption block is constituted by an initial vector (IV (Initial Vector)) the seed (Seed) and data E_{K_c} (data) that enciphered contents data by key K_c .

[0046] Key K_c is constituted by the value calculated to the hash function with the application of the value Seed set to the contents key K_c by random numbers as shown in a following formula.

[0047] $K_c = \text{Hash}(K_c \text{Seed})$ [0048] The initial vector IV and the seed Seed are set as a different value for every encryption block.

[0049] The data of contents is classified per 8 bytes and this encryption is performed every 8 bytes. 8 bytes of latter encryption is performed in the CBC (Cipher Block Chaining) mode performed using the result of 8 bytes of encryption of the preceding paragraph.

[0050] Since 8 bytes of encryption result of the preceding paragraph does not exist when enciphering 8 bytes of first contents data in the case of the CBC mode when enciphering 8 bytes of first contents data encryption is performed by making the initial vector IV into an initial value.

[0051] By performing encryption by this CBC mode even if one encryption block is decoded it is controlled that that influence attains to other encryption blocks.

[0052] About this encryption drawing 46 is made reference and explained in full detail behind.

[0053] About a cipher system it does not restrict to this.

[0054]The client 1 is no charge about the contents server 3 to contents as mentioned aboveand it can acquire freely. Thereforethe contents themselves become possible [distributing] in large quantities.

[0055]However each client 1 needs to hold the license when using the acquired contents. Then with reference to drawing 6 processing in case the client 1 reproduces contents is explained.

[0056]In Step S41 CPU21 of the client 1 acquires the identification information (CID) of the contents to which it pointed because a user operates the input part 26. This identification information is constituted by the title of contents the number given for each [which is memorized] contents of every etc. for example.

[0057]And CPU21 will read license ID (ID of a license required to use the contents) corresponding to the contents if contents are directed. This license ID is described by the header of the contents data enciphered as shown in drawing 5.

[0058]Next it is judged whether it progresses to Step S42 and the license corresponding to license ID read at Step S41 is already acquired by the client 1 and CPU21 is memorized by the storage parts store 28. When the license is not acquired it progresses to Step S43 and CPU21 still performs license acquisition processing. The details of this license acquisition processing are later mentioned with reference to the flow chart of drawing 7.

[0059]When judged with the license already being acquired in Step S42 Or in Step S43 as a result of performing license acquisition processing when a license is acquired it progresses to Step S44 and it is judged whether the license from which CPU21 is acquired is a thing within the term of validity. It is judged by comparing with the term (refer to drawing 8 mentioned later) specified as contents of the license and the present date clocked by the timer 20 whether a license is a thing within the term of validity. When judged with the term of validity of a license having already expired it progresses to Step S45 and CPU21 performs a license update process. The details of this license update process are later mentioned with reference to the flow chart of drawing 10.

[0060]When judged with a license being still within the term of validity in Step S44 Or when a license is updated it progresses to Step S46 and CPU21 reads the contents data enciphered from the storage parts store 28 and is made to store it in RAM23 in Step S45. And it is the encryption block unit arranged at the data of drawing 5 the data of the encryption block memorized by RAM23 is supplied to the encryption decoding part 24 and CPU21 makes it decode in Step S47 using the contents key Kc.

[0061]Although the example of the method of obtaining the contents key Kc is later mentioned with reference to drawing 15 Key K_{EKBC} contained in EKB (drawing 5) can be obtained using a device node key (DNK) (drawing 8) and the contents key Kc can be obtained from data K_{EKBC} (Kc) and (drawing 5) using the key K_{EKBC} .

[0062]CPU21 supplies the contents data decoded by the encryption decoding part 24 to the codec part 25 and makes it decode in Step S48 further. And from the input/output interface 32 CPU21 supplies the data decoded by the codec part 25 to the outputting part 27 carries out D/A conversion and makes it output from a

loudspeaker.

[0063] Next with reference to the flow chart of drawing 7 the details of the license acquisition processing performed at Step S43 of drawing 6 are explained.

[0064] The client 1 acquires the service information containing the pair of the leaves ID and DNK (Device Node Key) and the secret key and public key of the client 1 the public key of a license server and the certificate of each public key by registering with a license server a priori.

[0065] Leaf ID is a device node key required to express the identification information assigned for every client and for DNK decode the contents key Kc which is contained in EKB (validation key blocks) corresponding to the license and which is enciphered (with reference to drawing 12 it mentions later).

[0066] In Step S61 CPU21 acquires first URL corresponding to license ID made into the processing object now from the header shown in drawing 5. As mentioned above this URL is an address which should be accessed when acquiring the license corresponding to license ID too described by the header. Then in Step S62 CPU21 accesses URL acquired at Step S61. Specifically access is performed to the license server 4 by the communications department 29 via the Internet 2. At this time the license server 4 requires the input of the license specification information that the license (license required to use contents) to purchase is specified and user ID and a password from the client 1 (Step S102 of drawing 9 mentioned later). CPU21 displays this demand on the indicator of the outputting part 27. Based on this display a user operates the input part 26 and enters license specification information user ID and a password. The user of the client 1 accesses the license server 4 via the Internet 2 and acquires this user ID and password a priori.

[0067] In Step S63 and S64 CPU21 incorporates user ID and a password while incorporating the license identification information inputted from the input part 26. CPU21 makes the license request which controls the communications department 29 and contains the inputted user ID and leaf ID contained in license specification information and service information (it mentions later) in a password transmit to the license server 4 via the Internet 2 in Step S65.

[0068] the license server 4 is based on user ID a password and license specification information so that it may mention later with reference to drawing 9 -- a license -- transmitting (Step S109) -- or a license is not transmitted when conditions are not fulfilled (Step S112).

[0069] When it judges whether the license has been transmitted from the license server 4 and the license has been transmitted it progresses to Step S67 and CPU21 supplies the license to the storage parts store 28 and makes it memorize in Step S66.

[0070] In Step S66 when it judges with a license not being transmitted it progresses to Step S68 and CPU21 performs error handling. Since the license for using contents is not acquired specifically CPU21 forbids regeneration of contents.

[0071] It becomes possible to use the contents only after acquiring the license corresponding to license ID to which each client 1 accompanies contents data as mentioned above.

[0072]License acquisition processing of drawing 7 can also be beforehand carried out before each user acquires contents.

[0073]The license with which the client 1 is provided contains a service condition and leaf ID ****for example as shown in drawing 8.

[0074]The expiration date which can use contents for a service condition based on the licenseThe download term which can download contents based on the licenseThe number of times which can copy contents based on the license (copy frequency allowed)Based on the number of times of check-outthe number of times of the maximum check-outand its licenseThe information which shows the number of times which can copy contents to a right recordable on CD-R and PD (Portable Device)the right that a license can be shifted to ownership (acquisition state)duty to take a use loetc. is included.

[0075]Nextwith reference to the flow chart of drawing 9license offer processing of the license server 4 performed corresponding to the license acquisition processing of the client 1 of drawing 7 is explained. The composition of the client 1 of drawing 2 is quoted as composition of the license server 4 also in this case.

[0076]In Step S101CPU21 of the license server 4When it stands by until it received access from the client 1and access is receivedtransmission of user IDa passwordand license specification information is required from the client 1 which has progressed and accessed Step S102. As it mentioned aboveby processing of Step S65 of drawing 7 from the client 1. When user IDa password and leaf IDand license specification information (license ID) have been transmittedCPU21 of the license server 4 performs processing which receives and incorporates this via the communications department 29.

[0077]And in Step S103CPU21 of the license server 4 accesses the fee collection server 5 from the communications department 29and requires the crediting process of the user corresponding to user ID and a password. If the demand of a crediting process is received from the license server 4 via the Internet 2the fee collection server 5The payment history of the past of the user corresponding to the user ID and passwordetc. are investigatedWhen the credit result which permits grant of a license when it investigates whether there is any track record of the nonpayment of the remuneration of the user's license in the past and there is no such track record is transmitted and there are a track record of nonpaymentetc.the credit result of the disapproval of license granting is transmitted.

[0078]In Step S104CPU21 of the license server 4When it judges whether the credit result from the fee collection server 5 is a credit result which permits giving a license and grant of the license is permittedIt progresses to Step S105 and the license corresponding to the license specification information incorporated by processing of Step S102 is taken out out of the license memorized by the storage parts store 28. As for the license memorized by the storage parts store 28informationincluding license IDa versionthe date and time of creationthe term of validityetc.is described beforehand. In Step S106CPU21 adds leaf ID which received with the license. In Step S107CPU21 chooses the service condition

matched with the license selected at Step S105. Or by processing of Step S102 when a service condition is specified from a user the service condition is added to the service condition currently prepared beforehand again if needed. CPU21 adds the selected service condition to a license.

[0079] In Step S108 CPU21 signs a license with the secret key of a license server and thereby the license of composition as shown in drawing 8 is generated.

[0080] Next it progresses to Step S109 and CPU21 of the license server 4 makes the license (it has the composition shown in drawing 8) transmit to the client 1 via the Internet 2 from the communications department 29.

[0081] CPU21 of the license server 4 makes the storage parts store 28 memorize the license (a service condition and leaf ID are included) which is processing of Step S109 and transmitted now in Step S110 corresponding to the user ID and the password which were incorporated by processing of Step S102. In Step S111 CPU21 performs accounting. Specifically CPU21 requires the accounting to the user corresponding to the user ID and password of the fee collection server 5 from the communications department 29. The fee collection server 5 performs accounting to that user based on the demand of this fee collection. It can be licensed even if that user demands grant of a license henceforth when that user does not make payment to this accounting as mentioned above.

[0082] That is since the credit result which makes grant of a license disapproval from the fee collection server 5 is transmitted in this case it progresses to Step S112 from Step S104 and CPU21 performs error handling. CPU21 of the license server 4 outputs the message of the purport that a license cannot be given to the client 1 which controlled the communications department 29 and has accessed it and specifically terminates processing.

[0083] In this case since that client 1 cannot be licensed as mentioned above using those contents (decode a code) can be performed.

[0084] Drawing 10 expresses the details of the license update process in Step S45 of drawing 6. Processing of Step S131 of drawing 10 thru/or Step S135 is the fundamentally same processing as processing of Step S61 of drawing 7 thru/or Step S65. However in Step S133 CPU21 incorporates license ID of the license instead of the license to purchase to update. And in Step S135 CPU21 transmits user ID and license ID of the license updated with a password to the license server 4.

[0085] Corresponding to transmitting processing of Step S135 the license server 4 presents a service condition so that it may mention later (Step S153 of drawing 11). Then in Step S136 CPU21 of the client 1 receives presentation of the service condition from the license server 4 outputs this to the outputting part 27 and displays it. A user operates the input part 26 chooses a predetermined service condition out of this service condition or newly adds a predetermined service condition. CPU21 transmits the application for purchasing the service condition (conditions which update a license) selected as mentioned above to the license server 4 at Step S137. Corresponding to this application the license server 4 transmits a final service condition so that it may mention later (Step S154 of

drawing 11). Then in Step S138 CPU21 of the client 1 acquires the service condition from the license server 4 and updates the service condition in Step S139 as a service condition of the corresponding license already memorized by the storage parts store 28.

[0086] Drawing 11 expresses the license update process which the license server 4 performs corresponding to the license update process of the above client 1.

[0087] First in Step S151 in Step S152 CPU21 of the license server 4 will receive the license specification information which the client 1 transmitted at Step S135 with license update request information if access from the client 1 is received.

[0088] In Step S153 if the update request of a license is received CPU21 will read the service condition (service condition to update) corresponding to the license from the storage parts store 28 and will transmit to the client 1.

[0089] In [if it applies for the purchase of a service condition from the client 1 by processing of Step S137 of drawing 10 to this presentation as mentioned above] Step S154 CPU21 of the license server 4 generates the data corresponding to the service condition for which it applied and transmits to a client and 1 in Step S154. The client 1 updates the service condition of the already registered license using the service condition received by processing of Step S139 as mentioned above.

[0090] In this invention as shown in drawing 12 the key of a device and a license is managed based on the principle of a broadcasting yne KURIPUSHON (Broadcast Encryption) method. A key is made into a hierarchy tree structure and leaf (leaf) of the bottom corresponds to the key of each device. In the case of the example of drawing 12 16 devices from the number 0 to the number 15 or the key corresponding to a license is generated.

[0091] Each key is specified corresponding to each node of the tree structure shown by a figure Nakamaru seal. In the keys K00 thru/or K11 in this example the key K000 thru/or the key K111 correspond [corresponding to the root node of the highest rung / the route key KR / the key K0 and K1] corresponding to the node of the 4th step corresponding to the 3rd step of node respectively corresponding to the 2nd step of node. And the keys K0000 thru/or K1111 support the leaf (device node) as a node of the bottom respectively.

[0092] Since it is considered as the layered structure the key of the higher rank of the key K0010 and the key 0011 is set to K001 and the key of the higher rank of the key K000 and the key K001 is set to K00 for example. Like the following the key of the higher rank of the key K00 and the key K01 is set to K0 and the key of the higher rank of the key K0 and the key K1 is set to KR.

[0093] The key using contents is managed by the key corresponding to each node of one path from the device node (leaf) of the bottom to the root node of the highest rung. For example based on the license corresponding to the node (leaf ID) of the number 3 the key using contents is managed by each key of the path containing the key K0011K001K00K0 and KR.

[0094] In the system of this invention as shown in drawing 13 it is a keying system constituted based on the principle of drawing 12 and management of the key of a device and the key of a license is performed. In the example of drawing 13 8+24+32

steps of nodes are made into a tree structure and a category corresponds to each node from a root node to eight steps of a low rank. The category in here means categories such as a category of the apparatus which uses semiconductor memory such as a memory stick for example and a category of apparatus which receives digital broadcasting. And this system (T system is called) corresponds to one node in this category node as a system which manages a license.

[0095] That is a license corresponds by the key corresponding to 24 steps of a younger hierarchy's nodes further from the node of this T system. In the case of this example thereby the license of 2^{24} (about 16 mega) can be specified. 32 steps of lower hierarchies can prescribe the user (or client 1) of 2^{32} (about 4 giga). The key corresponding to 32 steps of nodes of the bottom constitutes DNK (Device Node Key) and ID corresponding to the leaf of the bottom is set to leaf ID.

[0096] Each device and the key of a license correspond to one of the paths which comprise each node of 64 (=8+24+32) stages. For example the contents key which enciphered contents is enciphered using the key corresponding to the node which constitutes the path assigned to the corresponding license. It is enciphered using the key of the hierarchy of the latest low rank and the key of the hierarchy of a higher rank is arranged in EKB (with reference to drawing 15 it mentions later).

DNK of the bottom is not arranged in EKB but is described by service information and is given to a user's client 1. the client 1 is described in EKB using the key which decoded the key of the hierarchy of the latest higher rank described in EKB (drawing 15) distributed with contents data using DNK described by the license and decoded and obtained it -- the key of the hierarchy on it is decoded to a pan. By performing the above processing one by one the client 1 can obtain all the keys belonging to the path of the license.

[0097] The concrete example of a classification of the category of a hierarchy tree structure is shown in drawing 14. In drawing 14 route key KR2301 is set to the highest rung of a hierarchy tree structure the node key 2302 is set to the following intermediate stages and the leaf key 2303 is set to the bottom. Each device holds each leaf key and a series of node keys from a leaf key to a route key and a route key.

[0098] The predetermined node of the Mth step (the example of drawing 13 M= 8) is set up as the category node 2304 from the highest rung. That is let each of the node of the Mth step be a device setting-out node of a specific category. Let M+1 or less step of node and a leaf be the node and leaf about the device contained in the category by making one node of the Mth step into the peak.

[0099] For example a category [memory stick (trademark)] is set to the one node 2305 of the Mth step of drawing 14 and the node which stands in a row below in this node and a leaf are set up as the node or leaf only for a category containing various devices which use memo RISUTEIKU. That is 2305 or less node is defined as the related node of the device defined as the category of a memory stick and a set of a leaf.

[0100] The low-ranking stage can be set up as the subcategory node 2306 by several steps from M stage. In the example of drawing 14 the node 2306 of [the

vessel only for reproduction] is set up as a subcategory node contained in the category of the device which uses a memory stick for the node under two steps of the category [memory stick] node 2305. To 2306 or less node of the vessel only for reproduction which is a subcategory node. The node 2307 of the telephone with a music reproduction function included in the category of the vessel only for playback is set up and the [PHS] node 2308 contained in the low rank at the category of a telephone with a music reproduction function and the [cellular-phone] node 2309 are set up further.

[0101] A category and a subcategory only not only in the kind of device for example A certain maker. It is possible to set up in arbitrary units (these are generically called an entity hereafter) such as the node which a content provider a settlement-of-accounts organization etc. manage uniquely i.e. a batch a jurisdiction unit or a providing service unit. For example if one category node is set up as a peak node only for game machine machine XYZ which a game machine machine maker sells. In the game machine machine XYZ which a maker sells the node key of the lower berth below the peak node Store become a leaf key possible to sell and Distribution of after that and enciphered content Or the validation key blocks (EKB) constituted by the node key below the peak node key and the leaf key in distribution of various keys and an update process are generated and distributed and distribution of available data is attained only to the device below a peak node.

[0102] Thus by considering the following nodes as the category defined as the peak node or the composition set up as a related node of a subcategory by making one node into the peak. The maker which manages one peak node of the category stage or the subcategory stage a content provider etc. generate uniquely the validation key blocks (EKB) which make the node the peak. The composition distributed to the device belonging to below a peak node is attained and renewal of a key can be performed without affecting at all the device belonging to the node of other categories which do not belong to a peak node.

[0103] For example in the tree structure shown in drawing 12 the four devices 012 and 3 contained in one group hold the key K00 common as a node key K0 and KR. By using this node key share composition it becomes possible to provide only the devices 012 and 3 with a common contents key. For example if node key K00 the very thing held in common is set up as a contents key setting out of a contents key only with the common devices 012 and 3 is possible without performing new key sending. If the value Enc (K00 Kcon) which enciphered the new contents key Kcon by the node key K00 is stored in a recording medium via a network and distributed to the devices 012 and 3. Only the devices 012 and 3 become possible [solving the code Enc (K00 Kcon) using the share node key K00 held in each device and obtaining the contents key Kcon]. It is shown that Enc (Ka Kb) is the data which enciphered Kb by Ka.

[0104] When it is revealed in t at a certain time that the key K0011 which the device 3 owns K001 K00 K0 and KR were analyzed by the aggressor (hacker) and it was exposed of KR. After it in order to protect the data transmitted and received by a system (group of the devices 012 and 3) it is necessary to separate the device 3

from a system. for that purpose -- a node key -- $K - 001 - K - 00 - K -$
 zero -- KR -- respectively -- being new -- a key -- $K - (-t -) - 001 - K -$
 $- (-t -) - 00 - K - (-t -) -$ zero -- $K - (-t -) - R$ -- updating -- a
 device -- zero -- one -- two -- the -- updating -- a key -- it is necessary to
 tell . Hereit is shown that $K(t)$ aaa is an updating key of the generation
 (Generation) t of the key K_{aaa} .

[0105]distribution **** of an updating key -- it ***** just. The renewal of a key
 the table constituted by the block data called the validation key blocks
 (EKB:EnablingKey Block) shown in drawing 15 Afor example via a networkOr it
 performs by storing in a recording medium and supplying the devices 01and 2.
 Validation key blocks (EKB) are constituted by the cryptographic key for
 distributing the key newly updated by the device corresponding to each leaf (node
 of the bottom) which constitutes a tree structure as shown in drawing 12.
 Validation key blocks (EKB) may be called the renewal block of a key (KRB:Key
 Renewal Block).

[0106]The validation key blocks (EKB) shown in drawing 15 A are constituted as
 block data with the data configuration which can update only the required device
 of renewal of a node key. In the devices 01and 2 in the tree structure shown in
drawing 12the example of drawing 15 A is the block data formed for the purpose of
 distributing the generation's t updating node key. drawing 12 -- from -- being
 clear -- as -- a device -- zero -- a device -- one -- updating -- a node key --
 ***** -- $K - (-t -) - 00 - K - (-t -) -$ zero -- $K - (-t -) - R -$
 $-$ required -- a device -- two -- updating -- a node key -- ***** -- $K - (-t -)$
 $-) - 001 - K - (-t -) - 00 - K - (-t -) -$ zero -- $K - (-t -) -$
 $R -$ being required .

[0107]As shown in EKB of drawing 15 Atwo or more cryptographic keys are
 contained in EKB. The cryptographic key of the bottom of drawing 15 A is Enc
 $(K0010K(t)001)$. this -- a device -- two -- having -- a leaf key -- $K - 0010 -$
 enciphering -- having had -- updating -- a node key -- $K - (-t -) - 001 -$
 it is -- a device -- two -- self -- having -- a leaf key -- $K - 0010 -$ this -- a
 cryptographic key -- decoding -- updating -- a node key -- $K - (-t -) - 001 -$
 -- it can obtain . using updating node key $K(t)001$ obtained by decodingdecoding of
 the 2nd step of cryptographic key Enc $(K - (-t -) - 001 - K - (-t -) -$
 $00)$ is attained from under drawing 15 Aand updating node key $K(t)00$ can be
 obtained.

[0108]One by one below by decoding the 2nd step of cryptographic key Enc $(K(t)$
 $00K(t)0)$ from on drawing 15 A. Updating node key $K(t)0$ is obtained and updating
 route key $K(t)R$ is obtained from on drawing 15 A using this by decoding the 1st
 step of cryptographic key Enc $(K(t)0$ and $K(t)R)$.

[0109]on the other hand -- a node key -- $K - 000 -$ updating -- an object --
 containing -- not having -- a node -- zero -- one -- updating -- a node key --
 ***** -- being required -- a thing -- $K - (-t -) - 00 - K - (-t -) -$
 zero -- $K - (-t -) - R -$ it is . The nodes 0 and 1 acquire updating node key
 $K(t)00$ from on drawing 15 A using the debye skiing $K0000$ and $K0001$ by decoding

the 3rd step of cryptographic key $\text{Enc}(K(t)0)$ below one by one updating node key $K(t)0$ is obtained by decoding the 2nd step of cryptographic key $\text{Enc}(K(t)0)$ from on drawing 15 A and updating route key $K(t)R$ is obtained by decoding the 1st step of cryptographic key $\text{Enc}(K(t)0)$ and $K(t)R$ from on drawing 15 A. Thus the devices 01 and 2 can obtain updated key $K(t)R$.

[0110] The index of drawing 15 A shows the actual address of the node key and leaf key which are used as a decryption key for decoding the cryptographic key on the right-hand side of a figure.

[0111] When renewal of node key $K(t)0$ and $K(t)R$ of the upper stage of the tree structure shown in drawing 12 is unnecessary and the update process of only the node key $K00$ is required. By using the validation key blocks (EKB) of drawing 15 B updating node key $K(t)00$ can be distributed to the devices 01 and 2.

[0112] EKB shown in drawing 15 B is available when distributing the new contents key shared for example in a specific group. As an example the recording medium with the devices 01 and 2 in the group who shows by a dotted line is used for drawing 12 and suppose that new common contents key $K(t)con$ is required. this -- the time -- a device -- zero -- one -- two -- three -- being common -- a node key -- $K(t)00$ -- having updated -- $K(t)00$ -- using -- being new -- being common -- updating -- a contents key -- $K(t)con$ -- having enciphered -- data -- $\text{Enc}(K(t)00K(t)con)$ -- drawing 15 B -- being shown -- having -- EKB -- distributing -- having . By this distribution the distribution as data of the device 4 etc. which other groups' apparatus cannot decode is attained.

[0113] That is if the devices 01 and 2 decode a cryptogram using key $K(t)00$ which processed and obtained EKB it will become possible to obtain contents key $K(t)con$ in time.

[0114] As an example of processing which obtains contents key $K(t)con$ in time to drawing 16 $K(t)$ Processing of the device 0 which received the data $\text{Enc}(K(t)00K(t)con)$ which enciphered new common contents key $K(t)con$ using $K00$ and EKB shown in drawing 15 B via the recording medium is shown. That is this example is an example which set the encryption message data based on EKB to contents key $K(t)con$.

[0115] As shown in drawing 16 the device 0 generates node key $K(t)00$ by same EKB processing with having mentioned above using EKB at the generation time stored in the recording medium and the node key $K000$ which he stores beforehand. Using updating node key $K(t)00$ decoded the device 0 decodes updating contents key $K(t)con$ and in order to use it behind by the leaf key $K0000$ which he has it enciphers and it stores it.

[0116] The example of a format of validation key blocks (EKB) is shown in drawing 17. The version 601 is an identifier which shows the version of validation key blocks (EKB). A version has the function to identify the newest EKB and a function which shows a correspondence relation with contents. A depth shows the hierarchy number of the hierarchy tree to the device of the distribution destination

of validation key blocks (EKB). The data pointer 603 is a pointer in which the position of the data division 606 in validation key blocks (EKB) is shown and is a pointer which the tag pointer 604 shows the position of the tag part 607 to and the signature pointer 605 shows the position of the signature 608.

[0117] The data division 606 stores the data which enciphered the node key updated for example. For example each cryptographic key about the updated node key as shown in drawing 16 is stored.

[0118] The tag part 607 is a tag in which the physical relationship of the node key and leaf key which were stored in the data division 606 and which were enciphered is shown. The grant rule of this tag is explained using drawing 18.

[0119] Drawing 18 shows the example which sends the validation key blocks (EKB) previously explained by drawing 15 A as data. The data at this time comes to be shown in the table of drawing 18 B. Let the address of the top node contained in the cryptographic key at this time be a top node address. Since updating key $K(t)$ R of the route key is contained in the case of this example a top node address serves as KR. At this time the data $\text{Enc}(K(t)0 \text{ and } K(t)R)$ of the highest rung corresponds to the position P0 shown in the hierarchy tree shown in drawing 18 A for example. The data of the following stage is $\text{Enc}(K(t)00K(t)0)$ and corresponds to the position P00 at the lower left of front data on a tree. When it sees from the position of a tree structure and data is in the bottom of it 0 and when there is nothing a tag is set as 1 for a tag. A tag is set up as {a left (L) tag and a right (R) tag}. Since there is data in the position P00 at the lower left of the position P0 corresponding to the data $\text{Enc}(K(t)0 \text{ and } K(t)R)$ of the highest rung of drawing 18 B and there is no data in L tag = 0 and the right it is set to R tag = 1. Hereafter a tag is set as all the data and the data row shown in drawing 18 C and a tag sequence are constituted.

[0120] A tag is set up in order that the corresponding data $\text{Enc}(K_{xxx}K_{yyy})$ may show where [of a tree structure] it is located. the key data $\text{Enc}(K_{xxx}K_{yyy})$ stored in the data division 606 -- although ... is only enumeration data of the key enciphered simply distinction of the position on the tree of the cryptographic key stored as data with the tag mentioned above of it is attained. The node index to which encryption data was made to correspond is used like composition of that previous drawing 15 explained without using the tag mentioned above for example it is 0: $\text{Enc}(K(t)0 \text{ and } K(t)R)$.

00: $\text{Enc}(K(t)00K(t)0)$

000: $\text{Enc}(K((t)000K(t)00)$

Although it is also possible to consider it as a data configuration like ...if it has composition using such an index in the distribution etc. which it becomes redundant data and data volume increases and pass a network it is not desirable. On the other hand distinction of a key position is attained with small data volume by using the tag mentioned above as index data in which a key position is shown.

[0121] It returns to drawing 17 and an EKB format is explained further. For example the signature (Signature) 608 published validation key blocks (EKB) it is an electronic signature which a lock management center (license server 4) contents

ROBAIDA (contents server 3) a settlement-of-accounts organization (fee collection server 5) etc. perform. It checks that the devices which received EKB are the validation key blocks (EKB) which the just validation key-blocks (EKB) publisher published by signature verification.

[0122] When processing using the contents supplied from the contents server 3 is summarized based on the license supplied from the license server 4 as mentioned above it comes to be shown in drawing 19.

[0123] That is while contents are provided from the contents server 3 to the client 1 a license is supplied to the client 1 from the license server 4. Contents are enciphered by the contents key Kc (Enc (KcContent)) and the contents key Kc It is added to the contents which were enciphered by the route key KR (it is a key obtained from EKB and corresponds to key K_{EKB} in drawing 5) (Enc (KRKc)) and were enciphered with EKB and is provided for the client 1.

[0124] As shown in drawing 20 the route key KR enciphered by DNK is contained in EKB in the example of drawing 19 for example (Enc (DNKKR)). Therefore the client 1 can obtain the route key KR from EKB using DNK contained in service information. The contents key Kc can be decoded from Enc (KRKc) using the route key KR and contents can be decoded from Enc (KcContent) using the contents key Kc.

[0125] Thus according to the principle explained with reference to drawing 12 and drawing 15 RIBOKU (revoke) of each client 1 becomes possible by assigning DNK individually to the client 1.

[0126] By adding and distributing license leaf ID in the client 1 matching of service information and a license will be performed and it becomes possible to prevent the illegal copy of a license.

[0127] It also enables an end user to create the contents which can prevent an illegal copy by distributing the certificate and secret key for clients as service information using these.

[0128] Use of a certificate and a secret key is later mentioned with reference to the flow chart of drawing 28.

[0129] In this invention since T system which manages a license and the category using various kinds of contents of a device are matched with a category node as explained with reference to drawing 13 two or more DNK(s) can be given to the same device. As a result it becomes possible to manage the contents of a different category with one device.

[0130] Drawing 21 expresses this relation. That is based on T system the license using the contents 1 to which DNK1 is assigned is recorded on the device D1. Similarly the contents 2 to which DNK2 was assigned and which carried out ripping to the memory stick from CD are recordable on this device D1 for example. In this case the device D1 becomes possible [treating simultaneously contents which are called the contents 1 and the contents 2 and which were distributed by a different system (T system and a device management system)]. Such a thing cannot be performed when assigning new DNK and DNK already assigned is deleted and it is made to make only one DNK correspond to a device.

[0131] By assigning the license category 1 and the license category 2 which are shown in drawing 22 at each of three square shapes each of 32 lower hierarchies [in / drawing 13] It becomes possible to classify the inside of the same category into small meetings such as a genre of contents, a label, a store, and a distribution service, and to manage it using a subcategory.

[0132] In the example of drawing 22, the license category 1 belongs to the genre of jazz, and the license category 2 belongs to the genre of a rock, for example. License ID makes the contents 1 and the contents 2 which are 1 correspond to the license category 1, and the user 1 thru/or the user 3 are supplied widely, respectively. The contents 3 of license ID 2, the contents 4, and the contents 5 are contained, and the user 1 and the user 3 are provided with the license category 2, respectively.

[0133] Thus, in this invention, the key management which became independent for every category becomes possible.

[0134] DNK is beforehand embedded to neither apparatus nor media, but by the license server 4, when performing registration processing, the system which can purchase the key by a user can be realized by making it download to each apparatus or media.

[0135] After it is created, content, even if what kind of usage is carried out, it is concerned with the usage, there are, and it is desirable in all the uses that it is usable. [no] For example, also in a different contents distribution service or the domain in which service conditions differ, it is desirable that the same contents can be used. In this invention, for this reason, as mentioned above, the certificate (certificates) of a secret key and the public key corresponding to it is distributed to each user (client 1) from the license server 4 as a certificate authority. Using the secret key, each user can create a signature (signature), can add to contents, and can guarantee genuine [of contents] (integrity), and can aim at prevention from an alteration of contents.

[0136] The example of processing in this case is explained with reference to the flow chart of drawing 23. Processing of drawing 23 explains the ripping processing a user makes the storage parts store 28, remember the data played from CD to be.

[0137] First, in Step S171, CPU21 of the client 1 incorporates the regenerative data of CD inputted via the communications department 29 as record data. In Step S172, CPU21 judges whether the watermark is contained in the record data incorporated by processing of Step S171. This watermark is constituted by the copy management information (CCI) of a triplet, and the 1-bit trigger (Trigger), and is embedded in the data of contents. It progresses to Step S173, and CPU21 performs processing which extracts the watermark when a watermark is detected. When a watermark does not exist, processing of Step S173 is skipped.

[0138] Next, in Step S174, CPU21 creates the data of the header recorded corresponding to contents. The data of this header is constituted by URL showing the access point for acquiring content ID, license ID, and a license, and the watermark.

[0139] Next, it progresses to Step S175, and CPU21 creates the digital signature based on the data of the header created by processing of Step S174 using its own secret key. This secret key is acquired from the license server 4 (Step S67 of

drawing 7).

[0140]CPU21 controls the encryption decoding part 24 by Step S176 and contents are made to encipher by a contents key. A contents key is simultaneously acquired when contents are acquired (drawing 5 or drawing 19).

[0141]Next for example CPU21 makes data record on the magneto-optical disc 43 constituted with a mini disc etc. in Step S177 based on a file format.

[0142]When a recording medium is a mini disc CPU21 supplies contents to the codec part 25 for example makes contents code with ATRAC3 method in Step S176. And the coded data is further enciphered by the encryption decoding part 24.

[0143]Drawing 24 expresses typically the state where contents were recorded on the recording medium as mentioned above. The watermark (WM) extracted from the contents (E (At3)) enciphered is recorded out of contents (header).

[0144]Drawing 25 expresses the more detailed composition of the file format in the case of recording contents on a recording medium. In this example content ID (CID) license ID (LID) URL and the header containing a watermark (WM) are recorded and also. EKB the data (Enc (KRKc)) which enciphered the contents key Kc by the route key KRA certificate (Cert) the digital signature (Sig (Header)) generated based on the header the data (Enc (KcContent)) which enciphered contents by the contents key Kc the metadata (Meta Data) and the mark (Mark) are recorded.

[0145]Although the watermark is embedded to the inside of contents As shown in drawing 24 and drawing 25 the inside of contents is making it arrange in a header independently and it becomes possible to detect the information currently embedded to contents as a watermark promptly and simply. Therefore it can be judged promptly whether the contents can be copied.

[0146]Metadata expresses the data of a jacket a photograph word set etc. for example. A mark is later mentioned with reference to drawing 31.

[0147]Drawing 26 expresses the example of the public key certification as a certificate. A public key certification is usually a certificate which the certificate authority (CA: Certificate Authority) in a public-key crypto system publishes. A certificate authority adds information including the term of validity etc. to self ID public key etc. which the user submitted to the certificate authority adds the digital signature by a certificate authority further to them and is created. In this invention since the license server 4 (or contents server 3) also publishes a certificate a secret key therefore a public key the user can get this public key certification by providing the license server 4 with user ID a password etc. and performing registration processing.

[0148]The consecutive numbers of the certificate in which the version number of a certificate and the license server 4 assign the public key certification in drawing 26 to the user (user) of a certificate. The algorithm used for the digital signature and a parameter the name of a certificate authority (license server 4) the term of validity of a certificate a certificate user's ID (node ID or leaf ID) and the certificate user's public key are contained as a message. The digital signature created by the license server 4 as a certificate authority is added to this message. This digital

signature is the data generated using the secret key of the license server 4 based on the hash value generated with the application of the hash function to the message.

[0149]in the case of the example of drawing 12if node ID or leaf ID is the device 0it will be set to "0000"if it comes out device 1it will be set to "0001"and if it is the device 15it will be set to "1111"for example. Based on such IDit is identified whether the device (entity) is an entity located in which position (a leaf or node) of tree composition.

[0150]Thusdistribution of contents will be freely performed by dissociating and distributing a license required to use contents with contents. The contents which came to hand in arbitrary methods or a course can be dealt with unitary.

[0151]By what a file format is constituted for as shown in drawing 25. When distributing the contents of the format via the Internetwhen it provides for SDMI (Secure Digital Music Initiative) apparatusof courseit becomes possible to manage the copyright of contents.

[0152]As shown in drawing 27 for exampleeven if contents are provided via a recording mediumEven if provided via the Internet 2the same processing enables it to check out to predetermined PD (Portable Device) as SDMI (Secure Digital Music Initiative) apparatusetc.

[0153]Nextwith reference to the flow chart of drawing 28processing in case the client 1 checks out contents to other clients (for examplePD) is explained.

[0154]Firstin Step S191CPU21 judges whether the digital signature is added to contents. When judged with the digital signature being addedit progresses to Step S192and CPU21 extracts a certificate and performs processing verified by the public key of a certificate authority (license server 4). That isthe client 1 acquires the public key corresponding to the secret key of the license server 4 to the license server 4and decodes the digital signature added to the public key certification by the public key. As explained with reference to drawing 26the digital signature is generated based on the secret key of a certificate authority (license server 4)and can be decoded using the public key of the license server 4. CPU21 calculates a hash value with the application of a hash function to the whole message of a certificate. And if CPU21 compares the calculated hash value with the hash value produced by decoding a digital signature and both are in agreementit will judge with a message not being what was altered. When both are not in agreementit will be said that this certificate is altered.

[0155]Thenin Step S193CPU21 judges whether the certificate is altered or notand when judged with not being alteredit progresses to Step S194 and it performs processing which verifies a certificate by EKB. This verification processing is performed by investigating whether EKB can be followed or not based on leaf ID (drawing 26) contained in a certificate. This verification is explained with reference to drawing 29 and drawing 30.

[0156]Nowas shown in drawing 29suppose that it is the device [RIBOKU / device / the device which has the leaf key K1001]. At this timedata (cryptographic key) as shown in drawing 30and EKB which has a tag are distributed to each device

(leaf). This EKB is EKB which updates the key KRK1K10 and K100 in order RIBOKU [the device "1001" in drawing 29].

[0157] All the leaves other than a RIBOKU device "1001" can acquire updated route key $K(t)R$. That is since the leaf which stands in a row in the low rank of the node key K0 holds in a device the node key K0 which is not updated it can acquire updating route key $K(t)R$ by decoding the cryptographic key $\text{Enc}(K0K(t)R)$ by the key K0.

[0158] The leaf not more than node key K11 can acquire updating node key $K(t)1$ using the node key K11 which is not updated by decoding $\text{Enc}(K11K(t)1)$ by the node key K11. It becomes possible by decoding $\text{Enc}(K(t)1$ and $K(t)R$ by node key $K(t)1$ to acquire updating route key $K(t)R$. Also about the low rank leaf of the node key K10 it is possible to acquire updating route key $K(t)R$ similarly.

[0159] The device "1000" which has the leaf key [RIBOKU / leaf key] $K1000\text{Enc}(K1000K(t)100)$ is decoded by the self leaf key K1000 node key $K(t)100$ can be acquired the node key of a higher rank can be further decoded one by one using this and updating route key $K(t)R$ can be acquired.

[0160] On the other hand -- RIBOKU -- having had -- a device -- "1001" -- self -- a leaf -- one -- a step -- a top -- updating -- a node key -- K -- (t) -- 100 -- EKB -- processing -- being unacquirable -- since -- after all -- updating -- a route -- a key -- K -- (t) -- R -- being unacquirable .

[0161] The data shown in drawing 30 and EKB which has a tag are distributed and stored in the just device [RIBOKU / device] (client 1) from the license server 4.

[0162] Then each client can perform EKB tracking processing using the tag. This EKB tracking processing is processing which judges whether a key distribution tree can be followed from the route key of a higher rank.

[0163] For example 1001 which is ID (leaf ID) of the leaf "1001" of drawing 29 is grasped as 4 bits of "1"00 and "1" and it is judged one by one from the most significant bit whether a tree can be followed according to a lower bit. In this judgment if a bit is 1 it will go to right-hand side and if it is 0 processing which goes to left-hand side will be performed.

[0164] Since the most significant bit of ID "1001" is 1 it goes to right-hand side from the route key KR of drawing 29. It is judged with the tag (tag of the number 0) of the beginning of EKB being 0: {00} and being what has data on both branches. In this case since it can go to right-hand side it can arrive at the node key K1.

[0165] Next it progresses to the node of the low rank of the node key K1. Since the 2nd bit of ID "1001" is 0 it goes to left-hand side. The tag in which the tag of the number 1 expresses the existence of the data of the low rank of the left-hand side node key K0 and the existence of the data of the low rank of the node key K1 is shown is a tag of the number 2. As shown in drawing 30 this tag shall be 2: {00} and shall have data on both branches. Therefore it can go to left-hand side and can arrive at the node key K10.

[0166] The 3rd bit of ID "1001" is 0 and goes to left-hand side. At this time the tag (tag of the number 3) in which the existence of the data of the low rank of K10 is shown is 3: {00} and it judges that it has data on both branches. Then it can go to

left-hand side and can arrive at the node key K100.

[0167]The least significant bit of ID "1001" is 1 and goes to right-hand side. The tag which the tag of the number 4 corresponds to the node key K11 and expresses the numerals of the data of the low rank of K100 is a tag of the number 5. This tag is 5: {01}. Therefore data will not exist in right-hand side. as a result arrive at a node "1001" — it is judged with there being nothing and the device of ID "1001" being the device which cannot acquire the updating route key by EKB i.e. a RIBOKU device.

[0168]On the other hand for example the device ID which has the leaf key K1000 is "1000" and like the case where it mentions above if EKB tracking processing based on the tag in EKB is performed it can arrive at a node "1000." Therefore it is judged with the device of ID "1000" being a just device.

[0169]Return to drawing 28 and CPU21 based on the verification processing of Step S194 When RIBOKU [***** / RIBOKU / the certificate / is judged at Step S195 and / the certificate] it progresses to Step S196 and processing which verifies a digital signature by the public key contained in a certificate is performed.

[0170]That is as shown in drawing 26 the certificate user's (contents creator) public key is contained in the certificate and the signature (Sig (Header)) shown in drawing 25 is verified using this public key. By namely the thing for which the data (hash value) produced by decoding the digital signature Sig (Header) is compared with the hash value calculated with the application of the hash function to Header shown in drawing 25 using this public key. It can check that Header is not altered if both are in agreement. On the other hand it will be said that Header is altered if both are not in agreement.

[0171]In Step S197 CPU21 judges whether Header is altered or not and if not altered it progresses to Step S198 and it verifies a watermark. In Step S199 CPU21 judges whether he can check out or not as a result of verification of a watermark. When you can check out it progresses to Step S200 and CPU21 performs check-out. That is contents are made to transmit and copy to the client 1 of a check-out place.

[0172]In [when judged with a digital signature not existing in Step S191] Step S193 In [when judged with the certificate being altered] Step S195 When are judged with the ability of a certificate to have not been verified by EKB and it is judged with the header being altered in Step S197 as a result of verification of a digital signature Or in Step S199 when judged with prohibition of check-out being described by the watermark it progresses to Step S201 and error handling is performed. That is check-out is forbidden in this case.

[0173]Thus it becomes possible by distributing a certificate and a secret key to a user from the license server 4 and adding a digital signature at the time of contents creation to guarantee Shinsei of the maker of contents. Thereby circulation of inaccurate contents can be controlled.

[0174]A watermark is detected at the time of contents creation by giving the information to a digital signature the alteration of watermark information can be prevented and Shinsei of contents can be guaranteed.

[0175]As a result even if the contents created once are distributed with what kind of gestalt it becomes possible to guarantee Shinsei of the original contents.

[0176]Since contents do not have a service condition but the service condition is added to the license it is changing the service condition within a license and it becomes possible to change the service conditions of the contents related to it all at once.

[0177]Next the utilizing method of a mark is explained. In this invention as mentioned above a service condition is added to the license instead of contents. However an operating condition may change with contents. Then in this invention as shown in drawing 25 a mark is added to contents.

[0178]Since a license and contents have one-pair Oshi's relation it becomes difficult to describe each operating condition of contents only in the service condition of a license. Then though management with a license is carried out by adding an operating condition to contents in this way it becomes possible to manage each contents.

[0179]As shown in drawing 31 a user's ID (leaf ID) an ownership flag beginning-of-using time copy frequency etc. are described by this mark for example.

[0180]The digital signature generated based on messages such as leaf ID an ownership flag beginning-of-using time and copy frequency is added to a mark.

[0181]An ownership flag is added when the license for which only a predetermined period makes contents usable is bought as it was for example (when duration of service is changed eternally). Beginning-of-using time is described when use of contents is started within a predetermined period. For example when the stage to download contents is restricted and download is performed within the term the time which downloaded contents actually is described here. Thereby it is proved that it is effective use within a period.

[0182]The number of times which copied the contents by then is described as a history (log) by copy frequency.

[0183]Next when a user buys a license with reference to the flow chart of drawing 32 a mark is explained as an example added to contents about the processing which adds a mark.

[0184]First in Step S221 CPU21 accesses the license server 4 via the Internet 2 based on instructions of the user from the input part 26.

[0185]In Step S222 CPU21 incorporates the input through the input part 26 from a user and requires acquisition of a license from the license server 4 corresponding to the input.

[0186]Corresponding to this demand the license server 4 presents a remuneration required in order to buy a license so that it may mention later with reference to the flow chart of drawing 33 (Step S242 of drawing 33). Then in Step S223 this will be outputted to the outputting part 27 and CPU21 of the client 1 will display it if presentation of the remuneration from the license server 4 is received.

[0187]A user judges whether based on this display it consents to the shown remuneration and inputs that decision result from the input part 26 based on that decision result.

[0188]When it judges with CPU21 having judged whether it consented to the remuneration shown the user in Step S224 based on the input from the input part 26 and having consented it progresses to Step S225 and processing which notifies consent to the license server 4 is performed.

[0189]If this notice of consent is received the license server 4 will transmit the information showing acquisition of a remuneration i.e. the mark which described the ownership flag (Step S244 of drawing 33). Then in Step S226 CPU21 of the client 1 will perform processing which embeds the received mark to contents in Step S227 if the mark from the license server 4 is received. That is the mark the ownership flag as shown in drawing 31 was described to be as a mark of the contents corresponding to the bought license by this will be recorded corresponding to contents. Since it means that the message was updated at this time CPU21 also updates a digital signature (drawing 25) and is recorded on a recording medium.

[0190]In Step S224 when judged with not consenting to the remuneration shown from the license server 4 it progresses to Step S228 and CPU21 notifies the license server 4 that it does not consent to the shown remuneration.

[0191]Corresponding to processing of such a client 1 the license server 4 performs processing shown in the flow chart of drawing 33.

[0192]Namely in Step S241 first CPU21 of the license server 4 if the demand of license acquisition is transmitted from the client 1 (Step S222 of drawing 32) this will be received a remuneration required for the acquisition by the target license will be read from the storage parts store 28 in Step S242 and this will be transmitted to the client 1.

[0193]As mentioned above the notice of whether to consent to the remuneration shown from the client 1 to the remuneration shown by doing in this way is transmitted.

[0194]Then in Step S243 CPU21 of the license server 4 when it judges whether the notice of consent was received from the client 1 and judges with having received the notice of consent progress to Step S244 generate the mark containing the message showing the acquisition by the target license and with its own secret key. A digital signature is added and it transmits to the client 1. Thus the transmitted mark is recorded on corresponding contents in the storage parts store 28 of the client 1 as mentioned above (Step S227 of drawing 32).

[0195]In Step S243 when judged with the notice of consent not being received from the client 1 processing of Step S244 is skipped. That is in this case since it means that acquisition processing of the license was not performed eventually a mark is not transmitted.

[0196]Drawing 34 expresses the example of composition of the mark transmitted from the license server 4 to the client 1 in Step S244. The mark is constituted in this example by digital signature Sig_s (LeafIDOwn) generated based on the secret key S of the license server 4 in leaf ID the ownership flag (Own) and that user's leaf ID and ownership flag.

[0197]Since this mark is effective only to a specific user's specific contents when

copied in the target contents the mark which accompanies those copied contents is repealed.

[0198] Thus contents and a license are separated and it becomes possible to realize service according to the operating condition of each contents also in the case where a service condition is made equivalent to a license.

[0199] Next a grouping is explained. It is called a grouping to collect two or more apparatus and media suitably and to enable it to deliver and receive contents freely in the one set. Usually this grouping is performed in apparatus and the media which an individual owns. Although this grouping set up the group key for every group and was performed conventionally it becomes possible to carry out a grouping easily by matching the same license with two or more apparatus and media which carry out grouping.

[0200] It is also possible to carry out the grouping of each apparatus by registering beforehand. The grouping in this case is explained below.

[0201] In this case the user needs to register into a server beforehand the certificate of the apparatus made into a grouping object. The registration processing of this certificate is explained with reference to the flow chart of drawing 35 and drawing 36.

[0202] First with reference to the flow chart of drawing 35 the registration processing of the certificate of a client (apparatus used as a grouping object) is explained. In Step S261 CPU21 of the client 1 draws up its own [as apparatus made into the object of a grouping] certificate. Its own public key is contained in this certificate.

[0203] Next it progresses to Step S262 and based on the input from a user's input part 26 CPU21 accesses the contents server 3 and performs processing which transmits the certificate drawn up by processing of Step S261 to the contents server 3 in Step S263.

[0204] As a certificate what received from the license server 4 can also be used as it is.

[0205] All the apparatus made into a grouping object performs the above processing.

[0206] Next with reference to the flow chart of drawing 36 the registration processing of the certificate of the contents server 3 performed corresponding to the registration processing of the certificate of the client 1 of drawing 35 is explained.

[0207] First in Step S271 in Step S272 CPU21 of the contents server 3 will register the certificate into the storage parts store 28 if the certificate transmitted from the client 1 is received.

[0208] The above processing is performed for every apparatus made into a group object. As a result as shown in drawing 37 the certificate of the device which constitutes the group is registered into the storage parts store 28 of the contents server 3 for every group for example.

[0209] In the example shown in drawing 37 the certificates C11 thru/or C14 are registered as the group's 1 certificate. Corresponding public key K_{P11} thru/or K_{P14}

is contained in these certificates C11 thru/or C14.

[0210] Similarly as the group's 2 certificate the certificates C21 thru/or C23 are registered and public key K_{p21} thru/or K_{p23} to which these correspond is contained.

[0211] If offer of contents is required of the apparatus which belongs to the group from a user in the state which constitutes the above groups where the certificate was registered for every apparatus the contents server 3 will perform processing shown in the flow chart of drawing 38.

[0212] First in Step S281 CPU21 of the contents server 3 performs processing which verifies the certificate which belongs to the group among the certificates memorized by the storage parts store 28.

[0213] This verification processing is performed by following EKB using a tag based on leaf ID contained in the certificate of each apparatus as explained with reference to drawing 29 and drawing 30. EKB is distributed also to the contents server 3 from the license server 4. The certificate [RIBOKU / certificate / this verification processing] is excepted.

[0214] In Step S282 CPU21 of the contents server 3 chooses the validated certificate as a result of the verification processing of Step S281. And in Step S283 CPU21 enciphers a contents key by each public key of the certificate of each apparatus selected by processing of Step S282. In Step S284 CPU21 transmits with contents the contents key enciphered by processing of Step S283 to each apparatus of the target group.

[0215] Supposing RIBOKU [the certificate C14] among the groups 1 by whom it is shown to drawing 37 it will be processing of Step S283 and encryption data as shown in drawing 39 will be generated for example.

[0216] That is the contents key K_c is enciphered by public key K_{p11} of the certificate C11 public key K_{p12} of the certificate C12 or public key K_{p13} of the certificate C13 in the example of drawing 39.

[0217] Corresponding to processing as shown in drawing 38 of the contents server 3 the apparatus (client) of each group who receives offer of contents performs processing shown in the flow chart of drawing 40.

[0218] First in Step S291 CPU21 of the client 1 receives the contents which the contents server 3 has transmitted by processing of Step S284 of drawing 38 with a contents key. Contents are enciphered by the contents key K_c and the contents key is enciphered by the public key which each apparatus holds as mentioned above (drawing 39).

[0219] Then in Step S292 CPU21 decodes and acquires the contents key addressed to it with its own secret key. [who received by processing of Step S291] And decoding processing of contents is performed using the acquired contents key.

[0220] For example using its own [corresponding to public key K_{p11}] secret key the apparatus corresponding to the certificate C11 shown in the example of drawing 39 decodes the code of the contents key K_c and acquires the contents key K_c . And contents are further decoded using the contents key K_c .

[0221] Same processing is performed also in the certificate C12 and the apparatus corresponding to C13. Since the contents key K_c enciphered using its own public

key is not sent along with contents the apparatus of the certificate [RIBOKU / certificate] C14 cannot decode the contents key Kc therefore cannot decode contents using the contents key Kc.

[0222] Although it was made to perform a grouping above to the contents key (namely contents) it is also possible to perform a grouping to a license key (license).

[0223] Grouping becomes possible without using a special group key and ICV (Integrity Check Value) mentioned later as mentioned above. This grouping is fit for applying to a small-scale group.

[0224] In this invention a license is also made possible [checking out checking in carrying out a move or copying]. However these processings are performed based on the rule defined by SDMI.

[0225] Next with reference to the flow chart of drawing 41 and drawing 42 check-out processing of the license by such a client is explained.

[0226] First processing of the client which checks out a license to other clients with reference to the flow chart of drawing 41 is explained. First in Step S301 CPU21 of the client 1 reads the number of times N1 of check-out of the license for check-out. Since this number of times of check-out is written in the service condition shown in drawing 8 it is read in this service condition.

[0227] Next in Step S302 CPU21 reads too the number of times N2 of the maximum check-out of the license for check-out in the service condition of a license.

[0228] And in Step S303 CPU21 The number of times N1 of check-out read by processing of Step S301 is compared with the number of times N2 of the maximum check-out read by processing of Step S302 and it is judged whether the number of times N1 of check-out is larger than the number of times N2 of the maximum check-out.

[0229] When it judges that the number of times N1 of check-out is smaller than the number of times N2 of the maximum check-out progress to Step S304 and CPU21 The leaf key of the device (client of a check-out place) of the other party is acquired from the device of partner each and the leaf key is stored in the check-out list of storage parts stores 28 corresponding to license ID made applicable to check-out now.

[0230] Next in Step S305 only 1 *****s the value of the number of times N1 of check-out of the license in which CPU21 was read by processing of Step S301. In Step S306 CPU21 calculates ICV based on the message of a license. This ICV is later mentioned with reference to drawing 46 thru/or drawing 50. It becomes possible to prevent the alteration of a license using ICV.

[0231] Next CPU21 enciphers using its own public key and makes ICV calculated by the license for check-out and processing of Step S306 output and copy to the device of the other party with EKB and a certificate in Step S307. CPU21 makes ICV calculated by processing of Step S306 remember it to be a leaf key of an opposite party device in the check list of the storage parts store 28 in Step S308 corresponding to license ID.

[0232] In Step S303 when judged with the number of times N1 of check-out not being smaller than the number of times N2 of the maximum check-out (for

example equal) since check-out is performed only the number of times already permitted cannot check out any more. Then it progresses to Step S309 and CPU21 performs error handling. That is check-out processing will be performed in this case.

[0233] Next with reference to the flow chart of drawing 42 check-out processing of drawing 41 explains processing of the client which receives check-out of a license.

[0234] First in Step S321 its own leaf key is transmitted to an opposite party device (client 1 which checks out a license). This leaf key is memorized by the client of the other party in Step S304 corresponding to license ID.

[0235] Next in Step S322 CPU21 receives this when the license and ICV which were enciphered from the client 1 of the other party have been transmitted with EKB and a certificate. That is this license ICV EKB and a certificate are transmitted from the device of the other party by processing of Step S307 of drawing 41.

[0236] CPU21 makes the storage parts store 28 memorize the license received by processing of Step S322 ICV EKB and a certificate in Step S323.

[0237] The client 1 which received check-out of the license as mentioned above performs processing shown in the flow chart of drawing 43 when using the license which received check-out and reproducing predetermined contents.

[0238] That is in Step S341 CPU21 of the client 1 calculates first ICV of the contents as which reproduction was specified by the user via the input part 26. And CPU21 makes ICV which is memorized by the storage parts store 28 and which is enciphered decode in Step S342 based on the public key contained in the certificate.

[0239] Next in Step S343 it is judged whether ICV calculated now by processing of Step S341 and ICV of CPU21 which was read by processing of Step S342 and decoded correspond. The license will be altered when both are in agreement. Then it progresses to Step S344 and CPU21 performs processing which reproduces corresponding contents.

[0240] On the other hand in Step S343 when judged with two ICV(s) not being in agreement a license has a possibility that it may be altered. For this reason it progresses to Step S345 and CPU21 performs error handling. That is at this time contents can be reproduced using that license.

[0241] Next processing of the client which receives check-in of the license once checked out to other clients as mentioned above is explained with reference to the flow chart of drawing 44.

[0242] First in Step S361 CPU21 acquires the leaf key of the device (client 1 which returns a license (check-in)) of the other party and ID of the license for check-in. Next in Step S362 CPU21 judges whether the license for [which was acquired at Step S361] check-in is a license which he checked out to the opposite party device. This judgment is performed based on ICV memorized by processing of Step S308 of drawing 41 a leaf key and license ID. That is when it is judged and memorized whether the leaf key acquired at Step S361 and the license ID and ICV are memorized during the check-out list it is judged with it being the license which he checked out.

[0243]In Step S363a license requires deletion of the license of the device of the other partyEKBand a certificate CPU21when he checks out. Based on this demandthe device of the other party performs deletion of a licenseEKBand a certificate so that it may mention later (Step S383 of drawing 45).

[0244]In Step S364since the once checked-out license has checked in at CPU21 againonly 1 carries out the decrement of the number of times N1 of check-out of the license.

[0245]In Step S365it is judged whether CPU21 has checked out other licenses to the device of the other partyWhen other licenses which he has still checked out do not existit progresses to Step S366 and CPU21 deletes the memory in the check-out list as check-in subject equipment of the device of the other party. On the other handin Step S365since check-in of other licenses may be received when judged with other licenses which he has checked out to the device of the other party existingprocessing of Step S366 is skipped.

[0246]In Step S362when it judges that the license made applicable to check-in is not a license which he checked out to the opposite party deviceit progresses to Step S367 and CPU21 performs error handling. That isin this casesince it will not be the license which he has jurisdiction overcheck-in processing is not performed.

[0247]when a user copies a license unjustlythe value of ICV memorized differs from the value of ICV calculated based on the license acquired by processing of Step S361 -- he can come out and check in.

[0248]Drawing 45 expresses processing of the client made to check in at the license which he has to the client which performs check-in processing of the license shown in the flow chart of drawing 44.

[0249]In Step S381CPU21 of the client 1 transmits ID of the license a leaf key and for check-in to the device (client 1 which performs processing shown in the flow chart of drawing 44) of the other party. As mentioned abovein Step S361the device of the other party acquires this leaf key and license IDand performs authenticating processing of the license for check-in in Step S362 based on it.

[0250]In Step S382CPU21 of the client 1 judges whether deletion of the license was required from the device of the other party. Namelywhen a license is a license for [just] check-inas mentioned aboveas for the device of the other partydeletion of a licenseEKBand a certificate is required by processing of Step S363. Thenwhen this demand is receivedit progresses to Step S383 and CPU21 deletes a licenseEKBand a certificate. That issince this client 1 will be in the state where that license cannot be used henceforth and DEKURI mend of the number of times N1 of check-out is carried out only for 1 by processing of Step S364 of drawing 44it means that check-in was completed by this.

[0251]In Step S382when judged with deletion of a license not being demanded from the device of the other partyit progresses to Step S384 and error handling is performed. That ischeck-in will not be possible for the reasons of the values of ICV differing in this case.

[0252]Although check-in and check-out were explained aboveit is possible similarly in a license a copy or for it to be made to carry out a move.

[0253]Next in order to prevent the alteration of a license (contents are also the same) the integrity check value (ICV) of a license is generated and it matches with a license and calculation of ICV explains the processing constitution which judges the existence of a license alteration.

[0254]The integrity check value (ICV) of a license is calculated for example using the hash function to a license and is calculated by $ICV = \text{hash}(\text{Kicv} \parallel L1 \parallel L2 \dots)$. Kicv is an ICV generation key. L1 and L2 are the information on a license and the message authenticator (MAC: Message authentication Code) of the critical information of a license is used.

[0255]The example of MAC value generation using DES cipher—processing composition is shown in drawing 46. (dividing the target message per 8 bytes as shown in the composition of drawing 46 — the divided message is hereafter set to) $M1 \parallel M2 \dots MN$ — exclusive OR of initial value (IV) and M1 is first carried out by operation part 24-1A (the result is set to I1). Next I1 is put into DES encryption section 24-1B and it enciphers using a key (hereafter referred to as K1) (an output is set to E1). Continuously exclusive OR of E1 and M2 is carried out by operation part 24-2A the output I2 is put in to DES encryption section 24-2B and it enciphers using the key K1 (output E2). Hereafter this is repeated and encryption processing is performed to all the messages. EN which came out at the last serves as a message authenticator (MAC (Message Authentication Code)) from DES encryption section 24-NB.

[0256]The integrity check value (ICV) of a license is generated by the MAC value and ICV generation key of such a license with the application of a hash function. For example if it will be guaranteed that there is no alteration in a license if ICV generated to the license generate time is compared with ICV newly generated based on the license and the same ICV is obtained and ICV(s) differ it will be judged with there having been an alteration.

[0257]Next the composition which sends Kicv which is an integrity check value (ICV) generation key of a license by above-mentioned validation key blocks is explained. That is it is the example used as the integrity check value (ICV) generation key of a license of the encryption message data based on EKB.

[0258]When a license common to two or more devices is sent to drawing 47 and drawing 48 the example of composition which distributes the integrity check value generation key Kicv for verifying the existence of an alteration of those licenses by validation key blocks (EKB) is shown. Drawing 47 shows the example which distributes the check value generation key Kicv which can be decoded to the devices 01 and 2 and drawing 48 shows the example which carries out RIBOKU (exclusion) of the devices 01 and 2 and the device 3 in three and distributes the check value generation key Kicv which can be decoded only to the devices 01 and 2.

[0259]In the example of drawing 47 by updating node key $K(t)_{00}$ with the data $\text{Enc}(K(t)_{00} \parallel \text{Kicv})$ which enciphered the check value generation key Kicv. a device — zero — one — two — three — setting — each — having — a node key — a leaf key — using — updating — having had — a node key — K — (— t —) — 00 —

decoding -- being possible -- validation -- key blocks (EKB) -- generating -- distributing . As shown in the right-hand side of drawing 47 first each device by processing EKB (decoding) updating -- having had -- a node key -- K -- (t) -- 00 -- acquiring -- next -- having acquired -- a node key -- K -- (t) -- 00 -- using -- enciphering -- having had -- a check -- a value -- generation -- a key -- $Enc(K(t)00Kicv)$ -- decoding -- a check -- a value -- generation -- a key -- $Kicv$ -- obtaining -- things -- being possible -- becoming .

[0260] the other devices 45 and 6 ... by the node key and leaf key which self holds even if it receives the same validation key blocks (EKB). Since node key $K(t)00$ which processed EKB and were updated are unacquirable a check value generation key can be safely sent only to a just device.

[0261] On the other hand the example of drawing 48 noting that RIBOKU (exclusion) of the device 3 is carried out by disclosure of the key in the group enclosed with the dotted-line frame of drawing 12 for example. It is other groups' Membai.e. the example which only received without the devices 01 and 2 and generated and distributed the validation key blocks (EKB) which can be decoded. The data $Enc(K(t)00Kicv)$ which enciphered the check value generation key ($Kicv$) as the validation key blocks (EKB) shown in drawing 48 by the node key ($K(t)00$) is distributed.

[0262] The decoding procedure is shown in the right-hand side of drawing 48. The devices 01 and 2 acquire an updating node key ($K(t)00$) from the received validation key blocks first by the decoding processing using the leaf key or node key which self holds. Next the check value generation key $Kicv$ is acquired by decoding by $K(t)00$.

[0263] the devices 45 and 6 of other groups who show drawing 12 -- even if ... receives this same data (EKB) it cannot acquire an updating node key ($K(t)00$) using the leaf key and node key which self holds. Also in the device [RIBOKU / device / similarly] 3 by the leaf key and node key which self holds an updating node key ($K(t)00$) cannot be acquired but only the device which has a just right becomes possible [decoding and using a check value generation key].

[0264] Thus if delivery of the check value generation key using EKB is used data volume will be lessened and only a just right holder will become possible [distributing the check value generation key whose decoding was enabled] safely.

[0265] The illegal copy of EKB and an encryption license can be eliminated by using the integrity check value (ICV) of such a license. For example as shown in drawing 49 there are the media 1 which stored the license L1 and the license L2 with the validation key blocks (EKB) which can acquire each license key and the case where this is copied to the media 2 as it was is assumed. The copy of EKB and an encryption license will be possible and this can be used with the device which can decode EKB.

[0266] In the example shown in drawing 49 Bit has composition which matches with the license justly stored in each media and stores an integrity check value (ICV (L1L2)). (ICV (L1L2)) shows $ICV = \text{hash}(KicvL1L2)$ which is an integrity check value of the license calculated by using a hash function for the license L1 and the

license L2. In the composition of drawing 49 B the license 1 and the license 2 are justly stored in the media 1 and the integrity check value (ICV (L1L2)) generated based on the license L1 and the license L2 is stored in them. The license 1 is justly stored in the media 2 and the integrity check value (ICV (L1)) generated based on the license L1 is stored in them.

[0267] Supposing it copies {EKB and the license 2} which were stored in the media 1 to the media 2 in this composition by the media 2. If a license check value is newly generated ICV (L1L2) will be generated and unlike Kicv (L1) stored in the media 2 it will become clear that storing of the new license by an alteration or the unjust copy of a license was performed. In the device which reproduces media an ICV check is performed to the front step of regeneration steps and coincidence of the generation ICV and the storing ICV is distinguished and when not in agreement it becomes possible to prevent reproduction of a license of an illegal copy by having composition which does not perform reproduction.

[0268] In order to improve safety it is good also as composition generated based on the data which rewrote the integrity check value (ICV) of the license and includes a counter. That is it has composition calculated by $ICV = \text{hash}(Kicv \text{ counter} + 1L1L2\dots)$. Here one counter (counter+1) per rewriting of ICV is set up as a value to *****. A counter value needs to have composition stored in a secure memory.

[0269] In the composition which cannot store the integrity check value (ICV) of a license in the same media as a license it is good also as composition which stores the integrity check value (ICV) of a license on media with another license.

[0270] For example when a license is stored in the media by which anti-copying policies such as the Read Only media and the usual MO are not taken if an integrity check value (ICV) is stored in the same media rewriting of ICV may be made by the inaccurate user and there is a possibility that the safety of ICV cannot be maintained. In such a case by storing ICV in the safe media on a host machine and having composition which uses ICV for copy control (for example check-in/check-out move) of a license safe management of ICV and the alteration check of a license are attained.

[0271] This example of composition is shown in drawing 50. The license 1 thru/or the license 3 are stored in the media 2201 from which anti-copying policies such as the Read Only media and the usual MO are not taken in drawing 50. It is the example which stored the integrity check value (ICV) about these licenses in the safe media 2202 on the host machine with which it is not permitted that a user accesses freely and prevented rewriting of the inaccurate integrity check value (ICV) by a user. If the device which is equipped with the media 2201 for example has PC which is a host machine and composition which performs the check of ICV in a server and judges reproductive propriety as such composition when it performs reproduction of the media 2201 reproduction of an unjust copy license or an alteration license can be prevented.

[0272] The client to which this invention is applied can be used as PDA (Personal Digital Assistants) a portable telephone a game terminal machine etc. in addition to

what is called a personal computer.

[0273]The computer by which the program which constitutes the software is included in hardware for exclusive use when performing a series of processings by softwareOr it is installed in the personal computer etc. which can perform various kinds of functionsfor exampleare general-purposeetc. from a network or a recording medium by installing various kinds of programs.

[0274]. As shown in drawing 2this recording medium is distributed apart from a device main frame in order to provide a user with a program. The magnetic disk 41 (a floppy disk is included) with which the program is recordedthe optical disc 42 (CD-ROM (Compact Disk – ReadOnly Memory).) . DVD (Digital Versatile Disk) is included. It is not only constituted by the package media which consist of the magneto-optical disc 43 (MD (Mini-Disk) is included) or the semiconductor memory 44butIt comprises ROM22 with which a user is provided in the state where it was beforehand included in the device main frame and on which the program is recordeda hard disk contained in the storage parts store 28etc.

[0275]In this specificationeven if the processing serially performed in accordance with an order that the step which describes the program recorded on a recording medium was indicated is not of course necessarily processed seriallyit also includes a parallel target or the processing performed individually.

[0276]In order for the program which performs processing relevant to security to prevent analyzing the processingit is desirable to encipher the program itself. For examplethe processing which performs cipher processing etc. can constitute the program as a tamper resistant module.

[0277]Since the license which carries out the utilization permission of the contents is specifiedthe information indicated to the header of contents may not be license ID which identifies a license uniquely. It is the information as which license ID specifies a license required for use of contents in the above-mentioned examplea certain license is the information which specifies the contents which permit useand it is the information which discriminates the license demanded by a license request from the client 1. The list of the various attribution information about the contents of contents is indicated to contentsand it may be made to indicate the conditional expression of the contents a utilization permission is carried out to a license by the license of. In this casethe attribution information included in contents is information which specifies the license to which use of those contents is permittedThe license is the information which specifies the contents which permit useand the conditional expression contained in a license serves as information from which license ID discriminates a license uniquely. When it does in this wayit becomes possible to match two or more licenses with one contentsand a license can be published flexibly.

[0278]In this specificationa system expresses the whole device constituted by two or more devices.

[0279]

[Effect of the Invention]According to the information processor of this invention and a methoda license serverand the programlike the above. It enables it to

distribute the enciphered data freely and by having enabled it to use contents by acquiring a license separately without barring circulation of contents copyright can be protected and a suitable usage fee can be collected.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram showing the composition of the contents providing system which applied this invention.

[Drawing 2] It is a block diagram showing the composition of the client of drawing 1.

[Drawing 3] It is a flow chart explaining the download processing of the contents of the client of drawing 1.

[Drawing 4] It is a flow chart explaining contents offer processing of the contents server of drawing 1.

[Drawing 5] It is a figure showing the example of the format in Step S26 of drawing 4.

[Drawing 6] It is a flow chart explaining contents playback processing of the client of drawing 1.

[Drawing 7] It is a flow chart explaining the details of the license acquisition processing of Step S43 of drawing 6.

[Drawing 8] It is a figure showing the composition of a license.

[Drawing 9] It is a flow chart explaining processing of license offer of the license server of drawing 1.

[Drawing 10] It is a flow chart explaining the details of the license update process in Step S45 of drawing 6.

[Drawing 11] It is a flow chart explaining the license update process of the license server of drawing 1.

[Drawing 12] It is a figure explaining the composition of a key.

[Drawing 13] It is a figure explaining a category node.

[Drawing 14] It is a figure showing the example of correspondence of a node and a device.

[Drawing 15] It is a figure explaining the composition of validation key blocks.

[Drawing 16] It is a figure explaining use of validation key blocks.

[Drawing 17] It is a figure showing the example of a format of validation key blocks.

[Drawing 18] It is a figure explaining the composition of the tag of validation key blocks.

[Drawing 19] It is a figure explaining the decoding processing of the contents using DNK.

[Drawing 20] It is a figure showing the example of validation key blocks.

[Drawing 21] It is a figure explaining the assignment to one device of two or more contents.

[Drawing 22] It is a figure explaining the category of a license.

[Drawing 23] It is a flow chart explaining ripping processing of a client.

[Drawing 24] It is a figure explaining the composition of a watermark.

[Drawing 25] It is a figure showing the example of a format of contents.

[Drawing 26] It is a figure showing the example of a public key certification.

[Drawing 27] It is a figure explaining distribution of contents.

[Drawing 28] It is a flow chart explaining check-out processing of the contents of a client.

[Drawing 29] It is a figure explaining the example which follows the validation key blocks by a tag.

[Drawing 30] It is a figure showing the example of composition of validation key blocks.

[Drawing 31] It is a figure explaining the composition of a mark.

[Drawing 32] It is a flow chart explaining license acquisition processing of a client.

[Drawing 33] It is a flow chart explaining license acquisition processing of a license server.

[Drawing 34] It is a figure showing the example of composition of a mark.

[Drawing 35] It is a flow chart explaining the registration processing of the certificate of a client.

[Drawing 36] It is a flow chart explaining the certificate registration processing of a contents server.

[Drawing 37] It is a figure showing the example of a group's certificate.

[Drawing 38] It is a flow chart explaining processing of a contents server in case the grouping is performed.

[Drawing 39] It is a figure showing the example of encryption of a contents key.

[Drawing 40] It is a flow chart explaining processing of the client belonging to a group.

[Drawing 41] It is a flow chart which explains to other clients processing of the client which checks out a license.

[Drawing 42] It is a flow chart explaining processing of the client which receives check-out of a license from other clients.

[Drawing 43] It is a flow chart explaining regeneration of the client which received check-out of the license.

[Drawing 44] It is a flow chart explaining processing of the client which receives check-in of a license from other clients.

[Drawing 45] It is a flow chart which explains to other clients processing of the client which checks in at a license.

[Drawing 46] It is a figure explaining generation of MAC.

[Drawing 47] It is a flow chart explaining the decoding processing of an ICV generation key.

[Drawing 48] It is a figure explaining other decoding processings of an ICV generation key.

[Drawing 49] It is a figure explaining management of the copy of the license by ICV.

[Drawing 50] It is a figure explaining management of a license.

[Description of Notations]

1-11-2 [A timer21CPUand 24 / An encryption decoding part25 codec partsand

26 / An input part 27 outputting parts and 28 / A storage parts store and 29 /
Communications department] A client the 2 Internet and 3 A contents server and 4
A license server 5 fee-collection server and 20

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-359616

(P2002-359616A)

(43) 公開日 平成14年12月13日 (2002. 12. 13)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
H 0 4 L 9/08		G 0 9 C 5/00	5 J 1 0 4
G 0 9 C 5/00		H 0 4 L 9/00	Z E C
H 0 4 L 9/00	Z E C		6 0 1 B
9/32			6 7 5 B

審査請求 未請求 請求項の数14 O L (全 35 頁)

(21) 出願番号 特願2002-28915(P2002-28915)

(22) 出願日 平成14年2月6日(2002. 2. 6)

(31) 優先権主張番号 特願2001-33114(P2001-33114)

(32) 優先日 平成13年2月9日(2001. 2. 9)

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願2001-94803(P2001-94803)

(32) 優先日 平成13年3月29日(2001. 3. 29)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 田中 浩一

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 河上 達

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

最終頁に続く

(54) 【発明の名称】 情報処理装置および方法、ライセンスサーバ、並びにプログラム

(57) 【要約】

【課題】 コンテンツの配布を自由に行うことができ、許可されたユーザのみがコンテンツを利用できるようにする。

【解決手段】 クライアントは暗号化されたコンテンツをコンテンツサーバから受け取る。コンテンツのヘッダにはそのコンテンツを利用するとき必要とされるライセンスを特定するためのライセンス特定情報が記述されており、クライアントはライセンス特定情報を元にライセンスサーバにライセンスを要求する。ライセンスサーバは、ライセンス要求を受け取ると、課金処理を行った後、該当するライセンスをクライアントに送信する。クライアントはライセンスを保持していることを条件として、コンテンツを復号し再生する。

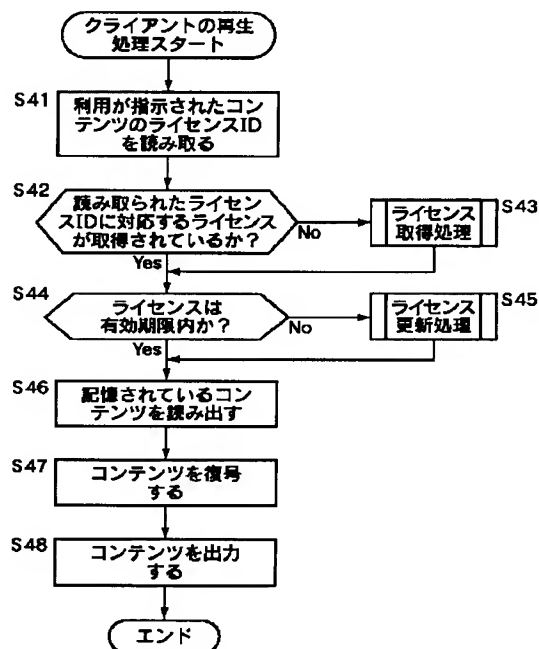


図6

【特許請求の範囲】

【請求項1】 ライセンスを保持していることを条件としてコンテンツの利用を許可する情報処理装置において、
当該コンテンツを利用許可する前記ライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを復号するために必要な鍵情報とを含む前記コンテンツを記憶するコンテンツ記憶手段と、
利用許可される前記コンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するライセンス記憶手段と、前記コンテンツを利用許可することができるライセンスが前記ライセンス記憶手段に記憶されているか否かを判定する判定手段と、
前記判定手段によりライセンスが記憶されていると判断されたことを条件として前記コンテンツのコンテンツデータを復号する復号手段とを備えることを特徴とする情報処理装置。

【請求項2】 前記情報処理装置は更に、
ライセンスサーバにライセンスを識別するためのライセンス識別情報を含むライセンス要求を送信する送信手段と、
ライセンスサーバによって送信されたライセンスを受信する受信手段とを備え、
前記受信手段により受信されたライセンスは前記ライセンス記憶手段に記憶されることを特徴とする請求項1記載の情報処理装置。

【請求項3】 前記コンテンツデータはテキストデータ、画像データ、音声データ、動画データあるいはそれらを組み合わせたデータであり、
前記復号手段により復号されたコンテンツデータを再生する再生手段を更に備えることを特徴とする請求項1記載の情報処理装置。

【請求項4】 前記鍵情報はEKB (Enabling Key Block) を含み、
前記情報処理装置は更にデバイスノードキーを記憶するデバイスノードキー記憶手段を備え、
前記復号手段は前記デバイスノードキー記憶手段に記憶されている前記デバイスノードキーを用いて前記EKB (Enabling Key Block) を復号処理し得られたルートキーを用いて前記暗号化されたコンテンツデータを復号することを特徴とする請求項1記載の情報処理装置。

【請求項5】 前記鍵情報は更に前記EKB (Enabling Key Block) のルートキーによって暗号化されたコンテンツキーを含み、
前記コンテンツデータは前記コンテンツキーにより暗号化されており、
前記復号手段は前記デバイスノードキー記憶手段に記憶されている前記デバイスノードキーを用いて前記EKB (Enabling Key Block) を復号処理し得られたルートキー

を用いて復号された前記コンテンツキーを用いて前記暗号化されたコンテンツデータを復号することを特徴とする請求項4記載の情報処理装置。

【請求項6】 前記ライセンスは更に、当該ライセンスによって利用可能となるコンテンツの使用条件を示す使用条件情報を含むことを特徴とする請求項1記載の情報処理装置。

【請求項7】 前記ライセンスは更に、ライセンスサーバの秘密鍵によりなされた電子署名を含むことを特徴とする請求項1記載の情報処理装置。

【請求項8】 前記情報処理装置は、更に情報処理装置を識別する端末識別情報を記憶する端末識別情報記憶手段を備え、前記ライセンス要求は更に、端末識別情報記憶手段に記憶されている前記端末識別情報を含み、
前記受信手段により受信された前記ライセンスは更に、前記端末識別情報を含み、
前記判定手段は、前記ライセンスに含まれる前記端末識別情報と前記端末識別情報記憶手段に記憶されている前記端末識別情報とを比較し、両者が一致している場合に限る、当該ライセンスを前記コンテンツの利用を許可できるライセンスであると判定することを特徴とする請求項2記載の情報処理装置。

【請求項9】 ライセンスを保持していることを条件としてコンテンツの利用を許可する情報処理方法であって、
当該コンテンツを利用許可する前記ライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを復号するために必要な鍵情報と、を含むコンテンツを記憶するステップと、
当該ライセンスによって利用許可される前記コンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するステップと、
前記コンテンツを利用許可することができるライセンスが前記ライセンス記憶手段に記憶されているか否かを判定するステップと、
前記判定手段によりライセンスが記憶されていると判断されたことを条件として前記コンテンツのコンテンツデータを復号するステップとを含むことを特徴とする情報処理方法。

【請求項10】 ライセンスを保持していることを条件としてコンテンツの利用を許可する処理をコンピュータに実行させるプログラムであって、
当該コンテンツを利用許可する前記ライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを復号するために必要な鍵情報と、を含むコンテンツを記憶するステップと、
当該ライセンスによって利用許可される前記コンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するステップと、
前記コンテンツを利用許可することができるライセンス

が前記ライセンス記憶手段に記憶されているか否かを判定するステップと、
前記判定手段によりライセンスが記憶されていると判断されたことを条件として前記コンテンツのコンテンツデータを復号するステップとをコンピュータに実行させるプログラム。

【請求項11】 前記プログラムあるいはその一部が暗号化されていることを特徴とする請求項10記載のプログラム。

【請求項12】 コンテンツの利用を許可するライセンスを発行するライセンスサーバにおいて、
当該ライセンスによって利用許可される前記コンテンツを特定するためのコンテンツ特定情報と、情報処理装置を識別する端末識別情報を含む前記ライセンスを記憶するライセンス記憶手段と情報処理装置から送信された、ライセンスを識別するライセンス識別情報を含むライセンス要求を受信する受信手段と、
前記ライセンス要求に含まれる前記ライセンス識別情報に対応する前記ライセンスを前記ライセンス記憶手段から抽出する抽出手段と、
前記抽出手段により抽出された前記ライセンスに前記端末識別情報を付加する処理手段と、
ライセンスサーバの秘密鍵を用いて、前記処理手段により端末識別情報を付加されたライセンスに電子署名を付加する署名手段と、
前記署名手段により署名されたライセンスを前記ライセンス要求を送信した情報処理装置に送信する送信手段とを備えることを特徴とするライセンスサーバ。

【請求項13】 コンテンツの利用を許可するライセンスを発行する情報処理方法であって、
当該ライセンスによって利用許可される前記コンテンツを特定するためのコンテンツ特定情報と、情報処理装置を識別する端末識別情報を含む前記ライセンスを記憶するステップと、
情報処理装置から送信された、ライセンスを識別するライセンス識別情報を含むライセンス要求を受信するステップと、
前記ライセンス要求に含まれる前記ライセンス識別情報に対応する前記ライセンスを前記ライセンス記憶手段から抽出するステップと、
前記抽出手段により抽出された前記ライセンスに前記端末識別情報を付加するステップと、
ライセンスサーバの秘密鍵を用いて、前記処理手段により端末識別情報を付加されたライセンスに電子署名を付加するステップと、
前記署名手段により署名されたライセンスを前記ライセンス要求を送信した情報処理装置に送信するステップとを含むことを特徴とする情報処理方法。

【請求項14】 コンテンツの利用を許可するライセンスを発行する処理処理をコンピュータに実行させるプロ

グラムであって、
当該ライセンスによって利用許可される前記コンテンツを特定するためのコンテンツ特定情報と、情報処理装置を識別する端末識別情報を含む前記ライセンスを記憶するステップと、
情報処理装置から送信された、ライセンスを識別するライセンス識別情報を含むライセンス要求を受信するステップと、
前記ライセンス要求に含まれる前記ライセンス識別情報に対応する前記ライセンスを前記ライセンス記憶手段から抽出するステップと、
前記抽出手段により抽出された前記ライセンスに前記端末識別情報を付加するステップと、
ライセンスサーバの秘密鍵を用いて、前記処理手段により端末識別情報を付加されたライセンスに電子署名を付加するステップと、
前記署名手段により署名されたライセンスを前記ライセンス要求を送信した情報処理装置に送信するステップとをコンピュータに実行させるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置および方法、ライセンスサーバ、並びにプログラムに関し、特に、著作権者からライセンスを受けていないコンテンツが不正にコピーされ、利用されるのを防止することができるようにした、情報処理装置および方法、ライセンスサーバ、並びにプログラムに関する。

【0002】

【従来の技術】最近、インターネットを介して、ユーザが、自分自身が保持している音楽データを他のユーザに提供し、自分自身が保持していない音楽データを他のユーザから提供を受けるようにして、複数のユーザが無料で音楽データを交換しあうシステムが実現されている。

【0003】このようなシステムでは、理論的には、1つの音楽、その他のコンテンツが存在すれば、他の全てのユーザが、それを利用することが可能となり、多くのユーザがコンテンツを購入しなくなるため、コンテンツに関する著作権者は、著作物としてのコンテンツが売れないため、著作物の販売に伴い、本来受け取ることが可能な著作物の利用に関するロイヤリティを受け取る機会を失うことになる。

【0004】

【発明が解決しようとする課題】そこで、コンテンツの流通を妨げることなく、不正に利用されることを防止することが、社会的に要請されている。

【0005】本発明はこのような状況に鑑みてなされたものであり、コンテンツが不正に利用されるのを確実に防止することができるようにするものである。

【0006】

【課題を解決するための手段】本発明の情報処理装置

は、コンテンツを利用許可するために必要なライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを復号するために必要な鍵情報とを含むコンテンツを記憶するコンテンツ記憶手段と、利用許可されるコンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するライセンス記憶手段と、コンテンツを利用許可することができるライセンスがライセンス記憶手段に記憶されているか否かを判定する判定手段と、判定手段によりライセンスが記憶されていると判断されたことを条件としてコンテンツのコンテンツデータを復号する復号手段とを備えることを特徴とする。

【0007】情報処理装置は更に、ライセンスサーバにライセンスを識別するためのライセンス識別情報を含むライセンス要求を送信する送信手段と、ライセンスサーバによって送信されたライセンスを受信する受信手段とを備え、受信手段により受信されたライセンスはライセンス記憶手段に記憶されるようにすることができる。

【0008】コンテンツデータはテキストデータ、画像データ、音声データ、動画データあるいはそれらを組み合わせたデータであり、復号手段により復号されたコンテンツデータを再生する再生手段を更に備えるようにすることができる。

【0009】鍵情報はEKB (Enabling Key Block) を含み、情報処理装置は更にデバイスノードキーを記憶するデバイスノードキー記憶手段を備え、復号手段はデバイスノードキー記憶手段に記憶されているデバイスノードキーを用いてEKB (Enabling Key Block) を復号処理し得られたルートキーを用いて暗号化されたコンテンツデータを復号するようすることができる。

【0010】鍵情報は更にEKB (Enabling Key Block) のルートキーによって暗号化されたコンテンツキーを含み、コンテンツデータはコンテンツキーにより暗号化されており、復号手段はデバイスノードキー記憶手段に記憶されているデバイスノードキーを用いてEKB (Enabling Key Block) を復号処理し得られたルートキーを用いて復号されたコンテンツキーを用いて暗号化されたコンテンツデータを復号するようすることができる。

【0011】ライセンスは更に、そのライセンスによって利用可能となるコンテンツの使用条件を示す使用条件情報を含むようすることができる。

【0012】ライセンスは更に、ライセンスサーバの秘密鍵によりなされた電子署名を含むようすることができる。

【0013】情報処理装置は、更に情報処理装置を識別する端末識別情報を記憶する端末識別情報記憶手段を備え、ライセンス要求は更に、端末識別情報記憶手段に記憶されている端末識別情報を含み、受信手段により受信されたライセンスは更に、端末識別情報を含み、判定手段は、ライセンスに含まれる端末識別情報と端末識別情

報記憶手段に記憶されている端末識別情報とを比較し、両者が一致している場合に限り、そのライセンスをコンテンツの利用を許可できるライセンスであると判定するようすることができる。

【0014】本発明の情報処理方法は、コンテンツを利用許可するライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを復号するために必要な鍵情報と、を含むコンテンツを記憶するステップと、利用許可されるコンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するステップと、コンテンツを利用許可することができるライセンスがライセンス記憶手段に記憶されているか否かを判定するステップと、判定手段によりライセンスが記憶されていると判断されたことを条件としてコンテンツのコンテンツデータを復号するステップとを含むことを特徴とする。

【0015】本発明のプログラムは、コンテンツを利用許可するライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを復号するために必要な鍵情報と、を含むコンテンツを記憶するステップと、利用許可されるコンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するステップと、コンテンツを利用許可することができるライセンスがライセンス記憶手段に記憶されているか否かを判定するステップと、判定手段によりライセンスが記憶されていると判断されたことを条件としてコンテンツのコンテンツデータを復号するステップとをコンピュータに実行させる。

【0016】プログラムあるいはその一部が暗号化されているようにすることができる。

【0017】本発明のライセンスサーバは、許可されるコンテンツを特定するためのコンテンツ特定情報と、情報処理装置を識別する端末識別情報を含むライセンスを記憶するライセンス記憶手段と、情報処理装置から送信された、ライセンスを識別するライセンス識別情報を含むライセンス要求を受信する受信手段と、ライセンス要求に含まれるライセンス識別情報に対応するライセンスをライセンス記憶手段から抽出する抽出手段と、抽出手段により抽出されたライセンスに端末識別情報を付加する処理手段と、ライセンスサーバの秘密鍵を用いて、処理手段により端末識別情報を付加されたライセンスに電子署名を付加する署名手段と、署名手段により署名されたライセンスをライセンス要求を送信した情報処理装置に送信する送信手段とを備えることを特徴とする。

【0018】本発明の情報処理方法は、利用許可されるコンテンツを特定するためのコンテンツ特定情報と、情報処理装置を識別する端末識別情報を含むライセンスを記憶するステップと、情報処理装置から送信された、ライセンスを識別するライセンス識別情報を含むライセンス要求を受信するステップと、ライセンス要求に含まれ

るライセンス識別情報に対応するライセンスをライセンス記憶手段から抽出するステップと、抽出手段により抽出されたライセンスに端末識別情報を付加するステップと、ライセンスサーバの秘密鍵を用いて、処理手段により端末識別情報を付加されたライセンスに電子署名を付加するステップと、署名手段により署名されたライセンスをライセンス要求を送信した情報処理装置に送信するステップとを含むことを特徴とする。

【0019】本発明の情報処理装置、情報処理方法、並びにプログラムでは、ライセンスを保持していることを条件としてコンテンツを復号し、利用可能にする。

【0020】本発明のライセンスサーバ、並びに情報処理方法では、特定の情報処理装置でのみ有効なライセンスを発行する。

【0021】

【発明の実施の形態】図1は、本発明を適用したコンテンツ提供システムの構成を示している。インターネット2には、クライアント1-1、1-2（以下、これらのクライアントを個々に区別する必要がある場合、単にクライアント1と称する）が接続されている。この例においては、クライアントが2台のみ示されているが、インターネット2には、任意の台数のクライアントが接続される。

【0022】また、インターネット2には、クライアント1に対してコンテンツを提供するコンテンツサーバ3、コンテンツサーバ3が提供するコンテンツを利用するのに必要なライセンスをクライアント1に対して付与するライセンスサーバ4、およびクライアント1がライセンスを受け取った場合に、そのクライアント1に対して課金処理を行う課金サーバ5が接続されている。

【0023】これらのコンテンツサーバ3、ライセンスサーバ4、および課金サーバ5も、任意の台数、インターネット2に接続される。

【0024】図2はクライアント1の構成を表している。

【0025】図2において、CPU（Central Processing Unit）21は、ROM（Read Only Memory）22に記憶されているプログラム、または記憶部28からRAM（Random Access Memory）23にロードされたプログラムに従って各種の処理を実行する。タイマ20は、計時動作を行い、時刻情報をCPU21に供給する。RAM23にはまた、CPU21が各種の処理を実行する上において必要なデータなども適宜記憶される。

【0026】暗号化復号部24は、コンテンツデータを暗号化するとともに、既に暗号化されているコンテンツデータを復号する処理を行う。コーデック部25は、例えば、ATRAC（Adaptive Transform Acoustic Coding）3方式などでコンテンツデータをエンコードし、入出力インタフェース32を介してドライブ30に接続されている半導体メモリ44に供給し、記録させる。あるいは

また、コーデック部25は、ドライブ30を介して半導体メモリ44より読み出した、エンコードされているデータをデコードする。

【0027】半導体メモリ44は、例えば、メモリスティック（商標）などにより構成される。

【0028】CPU21、ROM22、RAM23、暗号化復号部24、およびコーデック部25は、バス31を介して相互に接続されている。このバス31にはまた、入出力インタフェース32も接続されている。

【0029】入出力インタフェース32には、キーボード、マウスなどよりなる入力部26、CRT、LCDなどよりなるディスプレイ、並びにスピーカなどよりなる出力部27、ハードディスクなどより構成される記憶部28、モデム、ターミナルアダプタなどより構成される通信部29が接続されている。通信部29は、インターネット2を介しての通信処理を行う。通信部29はまた、他のクライアントとの間で、アナログ信号またはデジタル信号の通信処理を行う。

【0030】入出力インタフェース32にはまた、必要に応じてドライブ30が接続され、磁気ディスク41、光ディスク42、光磁気ディスク43、或いは半導体メモリ44などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部28にインストールされる。

【0031】なお、図示は省略するが、コンテンツサーバ3、ライセンスサーバ4、課金サーバ5も、図2に示したクライアント1と基本的に同様の構成を有するコンピュータにより構成される。そこで、以下の説明においては、図2の構成は、コンテンツサーバ3、ライセンスサーバ4、課金サーバ5などの構成としても引用される。

【0032】次に、図3のフローチャートを参照して、クライアント1がコンテンツサーバ3からコンテンツの提供を受ける処理について説明する。

【0033】ユーザが、入力部26を操作することでコンテンツサーバ3に対するアクセスを指令すると、CPU21は、ステップS1において、通信部29を制御し、インターネット2を介してコンテンツサーバ3にアクセスさせる。ステップS2において、ユーザが、入力部26を操作して、提供を受けるコンテンツを指定すると、CPU21は、この指定情報を受け取り、通信部29から、インターネット2を介してコンテンツサーバ3に、指定されたコンテンツを通知する。図4のフローチャートを参照して後述するように、この通知を受けたコンテンツサーバ3は、暗号化されたコンテンツデータを送信してくるので、ステップS3において、CPU21は、通信部29を介して、このコンテンツデータを受信すると、ステップS4において、その暗号化されているコンテンツデータを記憶部28を構成するハードディスクに供給し、記憶させる。

【0034】次に、図4のフローチャートを参照して、クライアント1の以上の処理に対応するコンテンツサーバ3のコンテンツ提供処理について説明する。なお、以下の説明において、図2のクライアント1の構成は、コンテンツサーバ3の構成としても引用される。

【0035】ステップS21において、コンテンツサーバ3のCPU21は、インターネット2から通信部29を介してクライアント1よりアクセスを受けるまで待機し、アクセスを受けたと判定したとき、ステップS22に進み、クライアント1から送信されてきたコンテンツを指定する情報を取り込む。このコンテンツを指定する情報は、クライアント1が、図3のステップS2において通知してきた情報である。

【0036】ステップS23において、コンテンツサーバ3のCPU21は、記憶部28に記憶されているコンテンツデータの中から、ステップS22の処理で取り込まれた情報で指定されたコンテンツを読み出す。CPU21は、ステップS24において、記憶部28から読み出されたコンテンツデータを、暗号化復号部24に供給し、コンテンツキーKcを用いて暗号化させる。

【0037】記憶部28に記憶されているコンテンツデータは、コーデック部25により、既にATRAC3方式によりエンコードされているので、このエンコードされているコンテンツデータが暗号化されることになる。

【0038】なお、もちろん、記憶部28に予め暗号化した状態でコンテンツデータを記憶させることができる。この場合には、ステップS24の処理は省略することが可能である。

【0039】次に、ステップS25において、コンテンツサーバ3のCPU21は、暗号化したコンテンツデータを伝送するフォーマットを構成するヘッダに、暗号化されているコンテンツを復号するのに必要なキー情報（図5を参照して後述するEKBとKEKBC(Kc)）と、コンテンツを利用するのに必要なライセンスを識別するためのライセンスIDを付加する。そして、ステップS26において、コンテンツサーバ3のCPU21は、ステップS24の処理で暗号化したコンテンツと、ステップS25の処理でキーとライセンスIDを付加したヘッダとをフォーマット化したデータを、通信部29から、インターネット2を介して、アクセスしてきたクライアント1に送信する。

【0040】図5は、このようにして、コンテンツサーバ3からクライアント1にコンテンツが供給される場合のフォーマットの構成を表している。同図に示されるように、このフォーマットは、ヘッダ(Header)とデータ(Data)とにより構成される。

【0041】ヘッダには、コンテンツ情報(Content information)、デジタル権利管理情報(DRM(Digital Right Management) information)、ライセンスID(License ID)、イネーブリングキーブロック(有効化キー

ブロック)(EKB(EnablingKey Block))および、EKBから生成されたキーKEKBCを用いて暗号化されたコンテンツキーKcとしてのデータKEKBC(Kc)が配置されている。なお、EKBについては、図15を参照して後述する。

【0042】コンテンツ情報には、データとしてフォーマット化されているコンテンツデータを識別するための識別情報としてのコンテンツID(CID)、そのコンテンツのコーデックの方式などの情報が含まれている。

【0043】デジタル権利管理情報には、コンテンツを使用する規則および状態(Usage rules/status)と、URL(Uniform Resource Locator)が配置されている。使用規則および状態には、例えば、コンテンツの再生回数、コピー回数などが記述される。

【0044】URLは、ライセンスIDで規定されるライセンスを取得するときアクセスするアドレス情報であり、図1のシステムの場合、具体的には、ライセンスを受けるために必要なライセンスサーバ4のアドレスである。ライセンスIDは、データとして記録されているコンテンツを利用するとき必要とされるライセンスを識別するものである。

【0045】データは、任意の数の暗号化ブロック(Encryption Block)により構成される。各暗号化ブロックは、イニシャルベクトル(IV(Initial Vector))、シード(Seed)、およびコンテンツデータをキーK'cで暗号化したデータE_{K'c}(data)により構成されている。

【0046】キーK'cは、次式により示されるように、コンテンツキーKcと、乱数で設定される値Seedをハッシュ関数に適用して演算された値により構成される。

【0047】 $K'c = \text{Hash}(Kc, \text{Seed})$

【0048】イニシャルベクトルIVとシードSeedは、各暗号化ブロック毎に異なる値に設定される。

【0049】この暗号化は、コンテンツのデータを8バイト単位で区分して、8バイト毎に行われる。後段の8バイトの暗号化は、前段の8バイトの暗号化の結果を利用して行われるCBC(Cipher Block Chaining)モードで行われる。

【0050】CBCモードの場合、最初の8バイトのコンテンツデータを暗号化するとき、その前段の8バイトの暗号化結果が存在しないため、最初の8バイトのコンテンツデータを暗号化するときは、イニシャルベクトルIVを初期値として暗号化が行われる。

【0051】このCBCモードによる暗号化を行うことで、1つの暗号化ブロックが解読されたとしても、その影響が、他の暗号化ブロックにおよぶことが抑制される。

【0052】なお、この暗号化については、図46を参照にして、後に詳述する。

【0053】また、暗号方式についてはこれに限らない。

【0054】以上のようにして、クライアント1は、コンテンツサーバ3からコンテンツを無料で、自由に取得することができる。従って、コンテンツそのものは、大量に、配布することが可能となる。

【0055】しかしながら、各クライアント1は、取得したコンテンツを利用するとき、ライセンスを保持している必要がある。そこで、図6を参照して、クライアント1がコンテンツを再生する場合の処理について説明する。

【0056】ステップS41において、クライアント1のCPU21は、ユーザが入力部26を操作することで指示したコンテンツの識別情報(CID)を取得する。この識別情報は、例えば、コンテンツのタイトルや、記憶されている各コンテンツ毎に付与されている番号などにより構成される。

【0057】そして、CPU21は、コンテンツが指示されると、そのコンテンツに対応するライセンスID(そのコンテンツを使用するのに必要なライセンスのID)を読み取る。このライセンスIDは、図5に示されるように、暗号化されているコンテンツデータのヘッダに記述されているものである。

【0058】次に、ステップS42に進み、CPU21は、ステップS41で読み取られたライセンスIDに対応するライセンスが、クライアント1により既に取得され、記憶部28に記憶されているか否かを判定する。まだ、ライセンスが取得されていない場合には、ステップS43に進み、CPU21は、ライセンス取得処理を実行する。このライセンス取得処理の詳細は、図7のフローチャートを参照して後述する。

【0059】ステップS42において、ライセンスが既に取得されていると判定された場合、または、ステップS43において、ライセンス取得処理が実行された結果、ライセンスが取得された場合、ステップS44に進み、CPU21は、取得されているライセンスは有効期限内のものであるか否かを判定する。ライセンスが有効期限内のものであるか否かは、ライセンスの内容として規定されている期限(後述する図8参照)と、タイマ20により計時されている現在日時と比較することで判断される。ライセンスの有効期限が既に満了していると判定された場合、CPU21は、ステップS45に進み、ライセンス更新処理を実行する。このライセンス更新処理の詳細は、図10のフローチャートを参照して後述する。

【0060】ステップS44において、ライセンスはまだ有効期限内であると判定された場合、または、ステップS45において、ライセンスが更新された場合、ステップS46に進み、CPU21は、暗号化されているコンテンツデータを記憶部28から読み出し、RAM23に格納させる。そして、ステップS47において、CPU21は、RAM23に記憶された暗号化ブロックのデータを、図5のデータに配置されている暗号化ブロック単位で、

暗号化復号部24に供給し、コンテンツキーKcを用いて復号させる。

【0061】コンテンツキーKcを得る方法の具体例は、図15を参照して後述するが、デバイスノードキー(DNK)(図8)を用いて、EKB(図5)に含まれるキーKEKBCを得ることができ、そのキーKEKBCを用いて、データKEKBC(Kc)(図5)から、コンテンツキーKcを得ることができる。

【0062】CPU21は、さらに、ステップS48において、暗号化復号部24により復号されたコンテンツデータをコーデック部25に供給し、デコードさせる。そして、コーデック部25によりデコードされたデータを、CPU21は、入出力インタフェース32から出力部27に供給し、D/A変換させ、スピーカから出力させる。

【0063】次に、図7のフローチャートを参照して、図6のステップS43で行われるライセンス取得処理の詳細について説明する。

【0064】クライアント1は、事前にライセンスサーバに登録することにより、リーフID、DNK(Device Node Key)、クライアント1の秘密鍵・公開鍵のペア、ライセンスサーバの公開鍵、及び各公開鍵の証明書を含むサーバデータを取得しておく。

【0065】リーフIDは、クライアント毎に割り当てられた識別情報を表し、DNKは、そのライセンスに対応するEKB(有効化キープブロック)に含まれる暗号化されているコンテンツキーKcを復号するのに必要なデバイスノードキーである(図12を参照して後述する)。

【0066】最初にステップS61において、CPU21は、いま処理対象とされているライセンスIDに対応するURLを、図5に示すヘッダから取得する。上述したように、このURLは、やはりヘッダに記述されているライセンスIDに対応するライセンスを取得するときアクセスすべきアドレスである。そこで、ステップS62において、CPU21は、ステップS61で取得したURLにアクセスする。具体的には、通信部29によりインターネット2を介してライセンスサーバ4にアクセスが行われる。このとき、ライセンスサーバ4は、クライアント1に対して、購入するライセンス(コンテンツを使用するのに必要なライセンス)を指定するライセンス指定情報、並びにユーザIDとパスワードの入力を要求してくる(後述する図9のステップS102)。CPU21は、この要求を出力部27の表示部に表示させる。ユーザは、この表示に基づいて、入力部26を操作して、ライセンス指定情報、ユーザID、およびパスワードを入力する。なお、このユーザIDとパスワードは、クライアント1のユーザが、インターネット2を介してライセンスサーバ4にアクセスし、事前に取得しておいたものである。

【0067】CPU21は、ステップS63、S64において、入力部26から入力されたライセンス識別情報を

取り込むとともに、ユーザIDとパスワードを取り込む。CPU 21は、ステップS 65において、通信部29を制御し、入力されたユーザIDとパスワードを、ライセンス指定情報及びサービスデータ（後述する）に含まれるリーフIDを含むライセンス要求をインターネット2を介してライセンスサーバ4に送信させる。

【0068】ライセンスサーバ4は、図9を参照して後述するように、ユーザIDとパスワード、並びにライセンス指定情報に基づいてライセンスを送信してくる（ステップS 109）か、または、条件が満たされない場合には、ライセンスを送信してこない（ステップS 112）。

【0069】ステップS 66において、CPU 21は、ライセンスサーバ4からライセンスが送信されてきたか否かを判定し、ライセンスが送信されてきた場合には、ステップS 67に進み、そのライセンスを記憶部28に供給し、記憶させる。

【0070】ステップS 66において、ライセンスが送信されて来ないと判定した場合、CPU 21は、ステップS 68に進み、エラー処理を実行する。具体的には、CPU 21は、コンテンツを利用するためのライセンスが得られないので、コンテンツの再生処理を禁止する。

【0071】以上のようにして、各クライアント1は、コンテンツデータに付随しているライセンスIDに対応するライセンスを取得して、初めて、そのコンテンツを使用することが可能となる。

【0072】なお、図7のライセンス取得処理は、各ユーザがコンテンツを取得する前に、予め行っておくようにすることも可能である。

【0073】クライアント1に提供されるライセンスは、例えば、図8に示されるように、使用条件、リーフIDおよびを含んでいる。

【0074】使用条件には、そのライセンスに基づいて、コンテンツを使用することが可能な使用期限、そのライセンスに基づいて、コンテンツをダウンロードすることが可能なダウンロード期限、そのライセンスに基づいて、コンテンツをコピーすることが可能な回数（許されるコピー回数）、チェックアウト回数、最大チェックアウト回数、そのライセンスに基づいて、コンテンツをCD-Rに記録することができる権利、PD（Portable Device）にコピーすることが可能な回数、ライセンスを所有権（買い取り状態）に移行できる権利、使用ログをとる義務等を示す情報が含まれる。

【0075】次に、図9のフローチャートを参照して、図7のクライアント1のライセンス取得処理に対応して実行されるライセンスサーバ4のライセンス提供処理について説明する。なお、この場合においても、図2のクライアント1の構成は、ライセンスサーバ4の構成として引用される。

【0076】ステップS 101において、ライセンスサ

ーバ4のCPU 21は、クライアント1よりアクセスを受けるまで待機し、アクセスを受けたとき、ステップS 102に進み、アクセスしてきたクライアント1に対して、ユーザIDとパスワード、並びに、ライセンス指定情報の送信を要求する。上述したようにして、クライアント1から、図7のステップS 65の処理で、ユーザIDとパスワード、リーフID並びにライセンス指定情報（ライセンスID）が送信されてきたとき、ライセンスサーバ4のCPU 21は、通信部29を介してこれを受信し、取り込む処理を実行する。

【0077】そして、ライセンスサーバ4のCPU 21は、ステップS 103において、通信部29から課金サーバ5にアクセスし、ユーザIDとパスワードに対応するユーザの与信処理を要求する。課金サーバ5は、インターネット2を介してライセンスサーバ4から与信処理の要求を受けると、そのユーザIDとパスワードに対応するユーザの過去の支払い履歴などを調査し、そのユーザが、過去にライセンスの対価の不払いの実績があるか否かなどを調べ、そのような実績がない場合には、ライセンスの付与を許容する与信結果を送信し、不払いの実績などがある場合には、ライセンス付与の不許可の与信結果を送信する。

【0078】ステップS 104において、ライセンスサーバ4のCPU 21は、課金サーバ5からの与信結果が、ライセンスを付与することを許容する与信結果であるか否かを判定し、ライセンスの付与が許容されている場合には、ステップS 105に進み、ステップS 102の処理で取り込まれたライセンス指定情報に対応するライセンスを、記憶部28に記憶されているライセンスの中から取り出す。記憶部28に記憶されているライセンスは、あらかじめライセンスID、バージョン、作成日時、有効期限等の情報が記述されている。ステップS 106において、CPU 21は、そのライセンスに受信したリーフIDを付加する。さらに、ステップS 107において、CPU 21は、ステップS 105で選択されたライセンスに対応づけられている使用条件を選択する。あるいはまた、ステップS 102の処理で、ユーザから使用条件が指定された場合には、その使用条件が必要に応じて、予め用意されている使用条件に付加される。CPU 21は、選択された使用条件をライセンスに付加する。

【0079】ステップS 108において、CPU 21はライセンスサーバの秘密鍵によりライセンスに署名し、これにより、図8に示されるような構成のライセンスが生成される。

【0080】次に、ステップS 109に進み、ライセンスサーバ4のCPU 21は、そのライセンス（図8に示される構成を有する）を、通信部29からインターネット2を介してクライアント1に送信させる。

【0081】ステップS 110においてライセンスサーバ4のCPU 21は、ステップS 109の処理で、いま送

信したライセンス（使用条件、リーフIDを含む）を、ステップS102の処理で取り込まれたユーザIDとパスワードに対応して、記憶部28に記憶させる。さらに、ステップS111において、CPU21は、課金処理を実行する。具体的には、CPU21は、通信部29から課金サーバ5に、そのユーザIDとパスワードに対応するユーザに対する課金処理を要求する。課金サーバ5は、この課金の要求に基づいて、そのユーザに対する課金処理を実行する。上述したように、この課金処理に対して、そのユーザが支払いを行わなかったような場合には、以後、そのユーザは、ライセンスの付与を要求したとしても、ライセンスを受けることができないことになる。

【0082】すなわち、この場合には、課金サーバ5からライセンスの付与を不許可とする返信結果が送信されてくるので、ステップS104からステップS112に進み、CPU21は、エラー処理を実行する。具体的には、ライセンスサーバ4のCPU21は、通信部29を制御してアクセスしてきたクライアント1に対して、ライセンスを付与することができない旨のメッセージを出力し、処理を終了させる。

【0083】この場合、上述したように、そのクライアント1はライセンスを受けることができないので、そのコンテンツを利用すること（暗号を復号すること）ができないことになる。

【0084】図10は、図6のステップS45におけるライセンス更新処理の詳細を表している。図10のステップS131乃至ステップS135の処理は、図7のステップS61乃至ステップS65の処理と基本的に同様の処理である。ただし、ステップS133において、CPU21は、購入するライセンスではなく、更新するライセンスのライセンスIDを取り込む。そして、ステップS135において、CPU21は、ユーザIDとパスワードとともに、更新するライセンスのライセンスIDを、ライセンスサーバ4に送信する。

【0085】ステップS135の送信処理に対応して、ライセンスサーバ4は、後述するように、使用条件を提示してくる（図11のステップS153）。そこで、クライアント1のCPU21は、ステップS136において、ライセンスサーバ4からの使用条件の提示を受信し、これを出力部27に出力し、表示させる。ユーザは、入力部26を操作して、この使用条件の中から所定の使用条件を選択したり、所定の使用条件を新たに追加したりする。ステップS137でCPU21は、以上のようにして選択された使用条件（ライセンスを更新する条件）を購入するための申し込みをライセンスサーバ4に送信する。この申し込みに対応して、後述するようにライセンスサーバ4は、最終的な使用条件を送信してくる（図11のステップS154）。そこで、ステップS138において、クライアント1のCPU21は、ライセンスサーバ4からの使用条件を取得し、ステップS139

において、その使用条件を記憶部28にすでに記憶されている対応するライセンスの使用条件として更新する。

【0086】図11は、以上のクライアント1のライセンス更新処理に対応して、ライセンスサーバ4が実行するライセンス更新処理を表している。

【0087】最初に、ステップS151において、ライセンスサーバ4のCPU21は、クライアント1からのアクセスを受けると、ステップS152において、クライアント1がステップS135で送信したライセンス指定情報をライセンス更新要求情報とともに受信する。

【0088】ステップS153において、CPU21は、ライセンスの更新要求を受信すると、そのライセンスに対応する使用条件（更新する使用条件）を、記憶部28から読み出し、クライアント1に送信する。

【0089】この提示に対して、上述したように、クライアント1から使用条件の購入が図10のステップS137の処理で申し込まれると、ステップS154において、ライセンスサーバ4のCPU21は、申し込まれた使用条件に対応するデータを生成し、ステップS154において、クライアント1に送信する。クライアント1は、上述したように、ステップS139の処理で受信した使用条件を用いて、すでに登録されているライセンスの使用条件を更新する。

【0090】本発明においては、図12に示されるように、ブロードキャストインクリプション（Broadcast Encryption）方式の原理に基づいて、デバイスとライセンスのキーが管理される。キーは、階層ツリー構造とされ、最下段のリーフ（leaf）が個々のデバイスのキーに対応する。図12の例の場合、番号0から番号15までの16個のデバイスまたはライセンスに対応するキーが生成される。

【0091】各キーは、図中丸印で示されるツリー構造の各ノードに対応して規定される。この例では、最上段のルートノードに対応してルートキーKRが、2段目のノードに対応してキーK0、K1が、3段目のノードに対応してキーK00乃至K11が、第4段目のノードに対応してキーK000乃至K111が、それぞれ対応されている。そして、最下段のノードとしてのリーフ（デバイスノード）に、キーK0000乃至K1111が、それぞれ対応されている。

【0092】階層構造とされているため、例えば、キーK0010とキー0011の上位のキーは、K001とされ、キーK000とキーK001の上位のキーは、K00とされている。以下同様に、キーK00とキーK01の上位のキーは、K0とされ、キーK0とキーK1の上位のキーは、KRとされている。

【0093】コンテンツを利用するキーは、最下段のデバイスノード（リーフ）から、最上段のルートノードまでの1つのパスの各ノードに対応するキーで管理される。例えば、番号3のノード（リーフID）に対応するラ

イセンスに基づき、コンテンツを利用するキーは、キーK0011, K001, K00, K0, KRを含むパスの各キーで管理される。

【0094】本発明のシステムにおいては、図13に示されるように、図12の原理に基づいて構成されるキーシステムで、デバイスのキーとライセンスのキーの管理が行われる。図13の例では、8+24+32段のノードがツリー構造とされ、ルートノードから下位の8段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そして、このカテゴリノードのうちの1つのノードに、ライセンスを管理するシステムとして本システム（Tシステムと称する）が対応する。

【0095】すなわち、このTシステムのノードよりさらに下の階層の24段のノードに対応するキーにより、ライセンスが対応される。この例の場合、これにより、2²⁴（約16メガ）のライセンスを規定することができる。さらに、最も下側の32段の階層により、2³²（約4ギガ）のユーザ（あるいはクライアント1）を規定することができる。最下段の32段のノードに対応するキーが、DNK（Device Node Key）を構成し、最下段のリーフに対応するIDがリーフIDとされる。

【0096】各デバイスやライセンスのキーは、64（=8+24+32）段の各ノードで構成されるパスの内の1つに対応される。例えば、コンテンツを暗号化したコンテンツキーは、対応するライセンスに割り当てられたパスを構成するノードに対応するキーを用いて暗号化される。上位の階層のキーは、その直近の下位の階層のキーを用いて暗号化され、EKB（図15を参照して後述する）内に配置される。最下段のDNKは、EKB内には配置されず、サービスデータに記述され、ユーザのクライアント1に与えられる。クライアント1は、ライセンスに記述されているDNKを用いて、コンテンツデータとともに配布されるEKB（図15）内に記述されている直近の上位の階層のキーを復号し、復号して得たキーを用いて、EKB内に記述されているさらにその上の階層のキーを復号する。以上の処理を順次行うことで、クライアント1は、そのライセンスのパスに属するすべてのキーを得ることができる。

【0097】図14に階層ツリー構造のカテゴリの分類の具体的な例を示す。図14において、階層ツリー構造の最上段には、ルートキーKR2301が設定され、以下の中間段にはノードキー2302が設定され、最下段には、リーフキー2303が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

【0098】最上段から第M段目（図13の例では、M=8）の所定のノードがカテゴリノード2304として

設定される。すなわち第M段目のノードの各々が特定カテゴリのデバイス設定ノードとされる。第M段の1つのノードを頂点としてM+1段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとされる。

【0099】例えば図14の第M段目の1つのノード2305にはカテゴリ「メモリスティック（商標）」が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード2305以下が、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義される。

【0100】さらに、M段から数段分下位の段をサブカテゴリノード2306として設定することができる。図14の例では、カテゴリ「メモリスティック」ノード2305の2段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、「再生専用器」のノード2306が設定されている。さらに、サブカテゴリノードである再生専用器のノード2306以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード2307が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる「PHS」ノード2308と、「携帯電話」ノード2309が設定されている。

【0101】さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば1つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器XYZ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器XYZに、その頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（EKB）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【0102】このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（EKB）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには

全く影響を及ぼさずにキー更新を実行することができる。

【0103】例えば、図12に示されるツリー構造において、1つのグループに含まれる4つのデバイス0, 1, 2, 3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、共通のコンテンツキーをデバイス0, 1, 2, 3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス0, 1, 2, 3のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーKconをノードキーK00で暗号化した値Enc(K00, Kcon)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kcon)を解いてコンテンツキーKconを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

【0104】また、ある時点tにおいて、デバイス3の所有する鍵K0011, K001, K00, K0, KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキーK001, K00, K0, KRを、それぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代（Generation）tの更新キーであることを示す。

【0105】更新キーの配布処理について説明する。キーの更新は、例えば、図15Aに示す有効化キープブロック（EKB: Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルを、ネットワークを介して、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。なお、有効化キープブロック（EKB）は、図12に示されるようなツリー構造を構成する各リーフ（最下段のノード）に対応するデバイスに、新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キープブロック（EKB）は、キー更新ブロック（KRB: Key Renewal Block）と呼ばれることもある。

【0106】図15Aに示す有効化キープブロック（EKB）は、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図15Aの例は、図12に示すツリー構造中のデバイス0, 1, 2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータであ

る。図12から明らかなように、デバイス0, デバイス1は、更新ノードキーとしてK(t)00、K(t)0、K(t)Rが必要であり、デバイス2は、更新ノードキーとしてK(t)001、K(t)00、K(t)0、K(t)Rが必要である。

【0107】図15AのEKBに示されるように、EKBには複数の暗号化キーが含まれる。図15Aの最下段の暗号化キーは、Enc(K0010, K(t)001)である。これはデバイス2の持つリーフキーK0010によって暗号化された更新ノードキーK(t)001であり、デバイス2は、自身の持つリーフキーK0010によってこの暗号化キーを復号し、更新ノードキーK(t)001を得ることができる。また、復号により得た更新ノードキーK(t)001を用いて、図15Aの下から2段目の暗号化キーEnc(K(t)001, K(t)00)が復号可能となり、更新ノードキーK(t)00を得ることができる。

【0108】以下順次、図15Aの上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号することで、更新ノードキーK(t)0が得られ、これを用いて、図15Aの上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号することで、更新ルートキーK(t)Rが得られる。

【0109】一方、ノードキーK000は更新する対象に含まれておらず、ノード0, 1が、更新ノードキーとして必要なのは、K(t)00、K(t)0、K(t)Rである。ノード0, 1は、デバイスキーK0000, K0001を用いて、図15Aの上から3段目の暗号化キーEnc(K0000, K(t)00)を復号することで更新ノードキーK(t)00を取得し、以下順次、図15Aの上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号することで、更新ノードキーK(t)0を得、図15Aの上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号することで、更新ルートキーK(t)Rを得る。このようにして、デバイス0, 1, 2は更新したキーK(t)Rを得ることができる。

【0110】なお、図15Aのインデックスは、図の右側の暗号化キーを復号するための復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0111】図12に示すツリー構造の上位段のノードキーK(t)0, K(t)Rの更新が不要であり、ノードキーK00のみの更新処理が必要である場合には、図15Bの有効化キープブロック（EKB）を用いることで、更新ノードキーK(t)00をデバイス0, 1, 2に配布することができる。

【0112】図15Bに示すEKBは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図12に点線で示すグループ内のデバイス0, 1, 2, 3がある記録

媒体を用いており、新たな共通のコンテンツキー

$K(t)con$ が必要であるとする。このとき、デバイス0, 1, 2, 3の共通のノードキー $K00$ を更新した $K(t)00$ を用いて新たな共通の更新コンテンツキー $K(t)con$ を暗号化したデータ $Enc(K(t)00, K(t)con)$ が、図15Bに示されるEKBとともに配布される。この配布により、デバイス4など、その他のグループの機器が復号することができないデータとしての配布が可能となる。

【0113】すなわち、デバイス0, 1, 2はEKBを処理して得たキー $K(t)00$ を用いて暗号文を復号すれば、 t 時点でのコンテンツキー $K(t)con$ を得ることが可能になる。

【0114】図16に、 t 時点でのコンテンツキー $K(t)con$ を得る処理例として、 $K(t)00$ を用いて新たな共通のコンテンツキー $K(t)con$ を暗号化したデータ $Enc(K(t)00, K(t)con)$ と、図15Bに示すEKBとを記録媒体を介して受領したデバイス0の処理を示す。すなわちこの例は、EKBによる暗号化メッセージデータをコンテンツキー $K(t)con$ とした例である。

【0115】図16に示すように、デバイス0は、記録媒体に格納されている世代 t 時点のEKBと、自分があるかじめ格納しているノードキー $K000$ を用いて、上述したと同様のEKB処理により、ノードキー $K(t)00$ を生成する。さらに、デバイス0は、復号した更新ノードキー $K(t)00$ を用いて、更新コンテンツキー $K(t)con$ を復号して、後にそれを使用するために自分だけが持つリーフキー $K0000$ で暗号化して格納する。

【0116】図17に有効化キーブロック(EKB)のフォーマット例を示す。バージョン601は、有効化キーブロック(EKB)のバージョンを示す識別子である。なお、バージョンは、最新のEKBを識別する機能と、コンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック(EKB)の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ603は、有効化キーブロック(EKB)中のデータ部606の位置を示すポインタであり、タグポインタ604はタグ部607の位置、署名ポインタ605は署名608の位置を示すポインタである。

【0117】データ部606は、例えば更新するノードキーを暗号化したデータを格納する。例えば図16に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【0118】タグ部607は、データ部606に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図18を用いて説明する。

【0119】図18では、データとして先に図15Aで

説明した有効化キーブロック(EKB)を送付する例を示している。この時のデータは、図18Bの表に示ようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この例の場合は、ルートキーの更新キー $K(t)R$ が含まれているので、トップノードアドレスはKRとなる。このとき、例えば最上段のデータ $Enc(K(t)0, K(t)R)$ は、図18Aに示す階層ツリーに示す位置P0に対応する。次の段のデータは、 $Enc(K(t)00, K(t)0)$ であり、ツリー上では前のデータの左下の位置P00に対応する。ツリー構造の所定の位置から見て、その下に、データがある場合は、タグが0、ない場合はタグが1に設定される。タグは{左(L)タグ, 右(R)タグ}として設定される。図18Bの最上段のデータ $Enc(K(t)0, K(t)R)$ に対応する位置P0の左下の位置P00にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図18Cに示すデータ列、およびタグ列が構成される。

【0120】タグは、対応するデータ $Enc(Kxxx, Kyyy)$ が、ツリー構造のどこに位置しているのかを示すために設定されるものである。データ部606に格納されるキーデータ $Enc(Kxxx, Kyyy) \cdots$ は、単純に暗号化されたキーの羅列データに過ぎないが、上述したタグによってデータとして格納された暗号化キーのツリー上の位置が判別可能となる。上述したタグを用いずに、先の図15で説明した構成のように、暗号化データに対応させたノード・インデックスを用いて、例えば、

0: $Enc(K(t)0, K(t)R)$

00: $Enc(K(t)00, K(t)0)$

000: $Enc(K(t)000, K(t)00)$

・・・のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると、冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【0121】図17に戻って、EKBフォーマットについてさらに説明する。署名(Signature)608は、有効化キーブロック(EKB)を発行した例えば鍵管理センタ(ライセンスサーバ4)、コンテンツサーバ3)、決済機関(課金サーバ5)等が実行する電子署名である。EKBを受領したデバイスは、署名検証によって正当な有効化キーブロック(EKB)を発行者が発行した有効化キーブロック(EKB)であることを確認する。

【0122】以上のようにして、ライセンスサーバ4から供給されたライセンスに基づいて、コンテンツサーバ3から供給されたコンテンツを利用する処理をまとめる

と、図19に示されるようになる。

【0123】すなわち、コンテンツサーバ3からクライアント1に対してコンテンツが提供されるとともに、ライセンスサーバ4からクライアント1にライセンスが供給される。コンテンツは、コンテンツキーKcにより、暗号化されており(Enc(Kc, Content))、コンテンツキーKcは、ルートキーKR(EKBから得られるキーであって、図5におけるキーKEKBcに対応する)で暗号化され(Enc(KR, Kc))、EKBとともに、暗号化されたコンテンツに付加されてクライアント1に提供される。

【0124】図19の例におけるEKBには、例えば、図20に示されるように、DNKで暗号化したルートキーKRが含まれている(Enc(DNK, KR))。従って、クライアント1は、サービスデータに含まれるDNKを利用して、EKBからルートキーKRを得ることができる。さらに、ルートキーKRを用いて、Enc(KR, Kc)からコンテンツキーKcを復号することができ、コンテンツキーKcを用いて、Enc(Kc, Content)からコンテンツを復号することができる。

【0125】このように、クライアント1にDNKを個別に割り当てることにより、図12と図15を参照して説明した原理に従って、個々のクライアント1のリボーク(revoke)が可能になる。

【0126】また、ライセンスリーフIDを付加して配布することにより、クライアント1において、サービスデータとライセンスの対応付けが行われることになり、ライセンスの不正コピーを防止することが可能になる。

【0127】また、クライアント用の証明書と秘密鍵をサービスデータとして配信するようにすることで、エンドユーザも、これらを用いて不正コピーを防止可能なコンテンツを作成することが可能になる。

【0128】証明書と秘密鍵の利用については、図28のフローチャートを参照して後述する。

【0129】本発明においては、図13を参照して説明したように、カテゴリノードにライセンスを管理するTシステムと、各種のコンテンツを利用するデバイスのカテゴリが対応づけられるので、複数のDNKを同一のデバイスに持たせることができる。その結果、異なるカテゴリのコンテンツを1つのデバイスで管理することが可能となる。

【0130】図21は、この関係を表している。すなわち、デバイスD1には、Tシステムに基づいて、DNK1が割り当てられている、コンテンツ1を利用するライセンスが記録される。同様に、このデバイスD1には、例えば、DNK2が割り当てられた、メモリスティックにCDからリッピングしたコンテンツ2を記録することができる。この場合、デバイスD1は、コンテンツ1とコンテンツ2という、異なるシステム(Tシステムとデバイス管理システム)により配信されたコンテンツを同時に扱うことが可能となる。新たなDNKを割り当てるとき、既

に割り当てられているDNKを削除するなどして、デバイスに1個のDNKだけを対応させるようにした場合、このようなことはできない。

【0131】また、図13における、例えば、下側の32階層の各三角形の1つ1つに、図22に示されるライセンスカテゴリ1とライセンスカテゴリ2を割り当てることにより、同一のカテゴリ内を、サブカテゴリを利用して、コンテンツのジャンル、レーベル、販売店、配信サービス等の小さな集まりに分類して、管理することが可能となる。

【0132】図22の例においては、例えば、ライセンスカテゴリ1は、ジャズのジャンルに属し、ライセンスカテゴリ2は、ロックのジャンルに属する。ライセンスカテゴリ1には、ライセンスIDが1であるコンテンツ1とコンテンツ2を対応させ、それぞれユーザ1乃至ユーザ3に配布されている。ライセンスカテゴリ2は、ライセンスID2のコンテンツ3、コンテンツ4、およびコンテンツ5が含まれ、それぞれユーザ1とユーザ3に提供されている。

【0133】このように、本発明においては、カテゴリ毎に独立したキー管理が可能になる。

【0134】また、DNKを、機器やメディアに予め埋め込むのではなく、ライセンスサーバ4により、登録処理を行う際に、各機器やメディアにダウンロードするようにすることで、ユーザによるキーの購入が可能なシステムを実現することができる。

【0135】コンテンツは、それが作成された後、どのような使われ方をされようとも、その使われ方に関わりなく、全ての用途において、使用可能であるのが望ましい。例えば、異なるコンテンツ配信サービス、あるいは使用条件が異なるドメインにおいても、同一のコンテンツが使えることが望ましい。本発明においては、このため、上述したように、各ユーザ(クライアント1)に、認証局としてのライセンスサーバ4から秘密鍵と、それに対応する公開鍵の証明書(certificates)が配布される。各ユーザは、その秘密鍵を用いて、署名(signature)を作成し、コンテンツに付加して、コンテンツの真正さ(integrity)を保証し、かつコンテンツの改竄防止を図ることができる。

【0136】この場合の処理の例について、図23のフローチャートを参照して説明する。図23の処理は、ユーザがCDから再生したデータを記憶部28に記憶させるリッピング処理を説明するものである。

【0137】最初に、ステップS171において、クライアント1のCPU21は、通信部29を介して入力されるCDの再生データを記録データとして取り込む。ステップS172において、CPU21は、ステップS171の処理で取り込まれた記録データにウォーターマークが含まれているか否かを判定する。このウォーターマークは、3ビットのコピー管理情報(CCI)と、1ビットの

トリガ (Trigger) とにより構成され、コンテンツのデータの中に埋め込まれている。CPU 21は、ウォーターマークが検出された場合には、ステップS173に進み、そのウォーターマークを抽出する処理を実行する。ウォーターマークが存在しない場合には、ステップS173の処理はスキップされる。

【0138】次に、ステップS174において、CPU 21は、コンテンツに対応して記録するヘッダのデータを作成する。このヘッダのデータは、コンテンツID、ライセンスID、ライセンスを取得するためのアクセス先を表すURL、およびウォーターマークにより構成される。

【0139】次に、ステップS175に進み、CPU 21は、ステップS174の処理で作成したヘッダのデータに基づいたデジタル署名を、自分自身の秘密鍵を用いて作成する。この秘密鍵は、ライセンスサーバ4から取得したものである (図7のステップS67)。

【0140】ステップS176で、CPU 21は、暗号化復号部24を制御し、コンテンツキーでコンテンツを暗号化させる。コンテンツキーは、コンテンツを取得したとき、同時に取得されたものである (図5または図19)。

【0141】次に、ステップS177において、CPU 21は、ファイルフォーマットに基づき、データを、例えば、ミニディスク等により構成される光磁気ディスク43に記録させる。

【0142】なお、記録媒体がミニディスクである場合、ステップS176において、CPU 21は、コンテンツをコーデック部25に供給し、例えば、ATRAC3方式によりコンテンツを符号化させる。そして、符号化されたデータが暗号化復号部24によりさらに暗号化される。

【0143】図24は、以上のようにして、記録媒体にコンテンツが記録された状態を模式的に表している。暗号化されているコンテンツ (E (At3)) から抽出されたウォーターマーク (WM) が、コンテンツの外 (ヘッダ) に記録されている。

【0144】図25は、コンテンツを記録媒体に記録する場合のファイルフォーマットのより詳細な構成を表している。この例においては、コンテンツID (CID)、ライセンスID (LID)、URL、およびウォーターマーク (WM) を含むヘッダが記録されている他、EKB、コンテンツキーKcをルートキーKRで暗号化したデータ (Enc (KR, Kc))、証明書 (Cert)、ヘッダに基づき生成されたデジタル署名 (Sig (Header))、コンテンツをコンテンツキーKcで暗号化したデータ (Enc (Kc, Content))、メタデータ (Meta Data) およびマーク (Mark) が記録されている。

【0145】ウォーターマークは、コンテンツの内部に埋め込まれているものであるが、図24と図25に示されるように、コンテンツの内部とは別に、ヘッダ内に配

置するようにすることで、ウォーターマークとしてコンテンツに埋め込まれている情報を迅速に、かつ簡単に検出することが可能となる。従って、そのコンテンツを、コピーすることができるか否かを、迅速に判定することができる。

【0146】なお、メタデータは、例えば、ジャケット、写真、歌詞等のデータを表す。マークについては、図31を参照して後述する。

【0147】図26は、証明書としての公開鍵証明書の例を表している。公開鍵証明書は、通常、公開鍵暗号方式における認証局 (CA: Certificate Authority) が発行する証明書であり、ユーザが、認証局に提出した自己のIDや公開鍵などに、認証局が有効期限等の情報を付加し、さらに、認証局によるデジタル署名を付加して作成される。この発行においては、ライセンスサーバ4 (またはコンテンツサーバ3) が、証明書と秘密鍵、従って公開鍵も発行するので、ユーザは、ユーザID、パスワード等をライセンスサーバ4に提供し登録処理を行うことによって、この公開鍵証明書を得ることができる。

【0148】図26における公開鍵証明書は、証明書のバージョン番号、ライセンスサーバ4が証明書の利用者 (ユーザ) に対して割りつける証明書の通し番号、デジタル署名に用いたアルゴリズム、およびパラメータ、認証局 (ライセンスサーバ4) の名前、証明書の有効期限、証明書利用者のID (ノードIDまたはリーフID)、並びに証明書利用者の公開鍵が、メッセージとして含まれている。さらに、このメッセージには、認証局としてのライセンスサーバ4により作成されたデジタル署名が付加されている。このデジタル署名は、メッセージに対してハッシュ関数を適用して生成されたハッシュ値に基づいて、ライセンスサーバ4の秘密鍵を用いて生成されたデータである。

【0149】ノードIDまたはリーフIDは、例えば、図12の例の場合、デバイス0であれば「0000」とされ、デバイス1であれば「0001」とされ、デバイス15であれば「1111」とされる。このようなIDに基づいて、そのデバイス (エンティティ) がツリー構成のどの位置 (リーフまたはノード) に位置するエンティティであるのかが識別される。

【0150】このように、コンテンツを利用するのに必要なライセンスを、コンテンツとは分離して配布するようにすることにより、コンテンツの配布が自由に行われることになる。任意の方法、あるいは経路で入手されたコンテンツは、一元的に取り扱うことが可能である。

【0151】また、ファイルフォーマットを図25に示されるように構成することで、そのフォーマットのコンテンツを、インターネットを介して配信する場合は勿論、SDMI (Secure Digital Music Initiative) 機器に提供する場合においても、コンテンツの著作権を管理することが可能となる。

【0152】さらに、例えば、図27に示されるように、コンテンツが記録媒体を介して提供されたとしても、インターネット2を介して提供されたとしても、同様の処理により、SDMI (Secure Digital Music Initiative) 機器としての所定のPD (Portable Device) 等に、チェックアウトしたりすることが可能となる。

【0153】次に、図28のフローチャートを参照して、クライアント1が他のクライアント (例えば、PD) に対してコンテンツをチェックアウトする場合の処理について説明する。

【0154】最初に、ステップS191において、CPU21は、コンテンツにデジタル署名が付加されているかを判定する。デジタル署名が付加されていると判定された場合、ステップS192に進み、CPU21は、証明書を抽出し、認証局 (ライセンスサーバ4) の公開鍵で検証する処理を実行する。すなわち、クライアント1は、ライセンスサーバ4からライセンスサーバ4の秘密鍵に対応する公開鍵を取得し、その公開鍵で公開鍵証明書に付加されているデジタル署名を復号する。図26を参照して説明したように、デジタル署名は、認証局 (ライセンスサーバ4) の秘密鍵に基づいて生成されており、ライセンスサーバ4の公開鍵を用いて復号することができる。さらに、CPU21は、証明書のメッセージ全体に対してハッシュ関数を適用してハッシュ値を演算する。そしてCPU21は、演算されたハッシュ値と、デジタル署名を復号して得られたハッシュ値とを比較し、両者が一致すれば、メッセージは改竄されたものではないと判定する。両者が一致しない場合には、この証明書は、改竄されたものであるということになる。

【0155】そこで、ステップS193において、CPU21は、証明書が改竄されていないかを判定し、改竄されていないと判定された場合、ステップS194に進み、証明書をEKBで検証する処理を実行する。この検証処理は、証明書に含まれるリーフID (図26) に基づいて、EKBをたどることができるかを調べることににより行われる。この検証について、図29と図30を参照して説明する。

【0156】いま、図29に示されるように、例えば、リーフキーK1001を有するデバイスがリボークされたデバイスであるとする。このとき、図30に示されるようなデータ (暗号化キー) とタグを有するEKBが、各デバイス (リーフ) に配布される。このEKBは、図29におけるデバイス「1001」をリボークするために、キーKR, K1, K10, K100を更新するEKBとなっている。

【0157】リボークデバイス「1001」以外の全てのリーフは、更新されたルートキーK(t)Rを取得することができる。すなわち、ノードキーK0の下位に連なるリーフは、更新されていないノードキーK0を、デバイス内に保持しているので、暗号化キーEnc(K0,

K(t)R)を、キーK0によって復号することで、更新ルートキーK(t)Rを取得することができる。

【0158】また、ノードキーK11以下のリーフは、更新されていないノードキーK11を用いて、Enc(K11, K(t)1)をノードキーK11によって復号することで、更新ノードキーK(t)1を取得することができる。さらに、Enc(K(t)1, K(t)R)をノードキーK(t)1によって復号することで、更新ルートキーK(t)Rを取得することが可能となる。ノードキーK101の下位リーフについても、同様に更新ルートキーK(t)Rを取得することが可能である。

【0159】さらに、リボークされていないリーフキーK1000を有するデバイス「1000」は、自己のリーフキーK1000でEnc(K1000, K(t)100)を復号して、ノードキーK(t)100を取得することができ、これを用いてさらに、上位のノードキーを順次復号し、更新ルートキーK(t)Rを取得することができる。

【0160】これに対して、リボークされたデバイス「1001」は、自己のリーフの1段上の更新ノードキーK(t)100を、EKB処理により取得できないので、結局、更新ルートキーK(t)Rを取得することができない。

【0161】リボークされていない正当なデバイス (クライアント1) には、図30に示されるデータとタグを有するEKBが、ライセンスサーバ4から配信され、格納されている。

【0162】そこで、各クライアントは、そのタグを利用して、EKB追跡処理を行うことができる。このEKB追跡処理は、上位のルートキーからキー配信ツリーをたどれるかを判定する処理である。

【0163】例えば、図29のリーフ「1001」のID (リーフID) である「1001」を、「1」「0」

「0」「1」の4ビットとして把握し、最上位ビットから順次、下位ビットに従って、ツリーをたどることができるかを判定される。この判定では、ビットが1であれば、右側に進み、0であれば、左側に進む処理が行われる。

【0164】ID「1001」の最上位ビットが1であるから、図29のルートキーKRから右側に進む。EKBの最初のタグ (番号0のタグ) は、0: {0, 0} であり、両枝にデータを有するものであると判定される。この場合、右側に進むことができるので、ノードキーK1にたどり着くことができる。

【0165】次に、ノードキーK1の下位のノードに進む。ID「1001」の2番目のビットは0であるから左側に進む。番号1のタグは、左側のノードキーK0の下位のデータの有無を表すものであり、ノードキーK1の下位のデータの有無を示すタグは、番号2のタグである。このタグは、図30に示されるように、2: {0,

0}であり、両枝にデータを有するものとされる。従って、左側に進み、ノードキーK10にたどり着くことができる。

【0166】さらに、ID「1001」の3番目のビットは0であり、左側に進む。このとき、K10の下位のデータの有無を示すタグ(番号3のタグ)は、3:{0,0}であり、両枝にデータを有するものと判定される。そこで、左側に進み、ノードキーK100にたどり着くことができる。

【0167】さらに、ID「1001」の最下位ビットは1であり、右側に進む。番号4のタグは、ノードキーK11に対応するものであり、K100の下位のデータの符号を表すタグは、番号5のタグである。このタグは、5:{0,1}である。従って、右側には、データが存在しないことになる。その結果、ノード「1001」にはたどり着けないことになり、ID「1001」のデバイスは、EKBによる更新ルートキーを取得できないデバイス、すなわちリボークデバイスであると判定される。

【0168】これに対して、例えば、リーフキーK1000を有するデバイスIDは、「1000」であり、上述した場合と同様に、EKB内のタグに基づくEKB追跡処理を行うと、ノード「1000」にたどり着くことができる。従って、ID「1000」のデバイスは、正当なデバイスであると判定される。

【0169】図28に戻って、CPU21は、ステップS194の検証処理に基づき、証明書がリボークされていないか否かをステップS195で判定し、証明書がリボークされていない場合には、ステップS196に進み、デジタル署名を証明書に含まれる公開鍵で検証する処理を実行する。

【0170】すなわち、図26に示されるように、証明書には、証明書利用者(コンテンツ作成者)の公開鍵が含まれており、この公開鍵を用いて、図25に示される署名(Sig(Header))が検証される。すなわち、この公開鍵を用いて、デジタル署名Sig(Header)を復号して得られたデータ(ハッシュ値)と、図25に示されるHeaderにハッシュ関数を適用して演算されたハッシュ値とを比較することで、両者が一致していれば、Headerが改竄されていないことを確認することができる。これに対して、両者が一致しなければ、Headerは改竄されているということになる。

【0171】ステップS197において、CPU21は、Headerが改竄されているか否かを判定し、改竄されていなければ、ステップS198に進み、ウォーターマークを検証する。ステップS199において、CPU21は、ウォーターマークの検証の結果、チェックアウトが可能であるか否かを判定する。チェックアウトが可能である場合には、ステップS200に進み、CPU21は、チェックアウトを実行する。すなわち、チェックアウト先のクライアント1に対してコンテンツを転送し、コピーさ

せる。

【0172】ステップS191において、デジタル署名が存在しないと判定された場合、ステップS193において、証明書が改竄されていると判定された場合、ステップS195において、証明書をEKBで検証することができなかったと判定された場合、ステップS197において、デジタル署名の検証の結果、ヘッダが改竄されていると判定された場合、または、ステップS199において、ウォーターマークにチェックアウトの禁止が記述されていると判定された場合、ステップS201に進み、エラー処理が実行される。すなわち、この場合には、チェックアウトが禁止される。

【0173】このように、証明書と秘密鍵をライセンスサーバ4からユーザに配布し、コンテンツ作成時に、デジタル署名を付加することにより、コンテンツの作成者の真正を保証することが可能となる。これにより、不正なコンテンツの流通を抑制することができる。

【0174】さらに、ウォーターマークをコンテンツ作成時に検出し、その情報をデジタル署名に付することで、ウォーターマーク情報の改竄を防止し、コンテンツの真正を保証することができる。

【0175】その結果、一度作成されたコンテンツは、どのような形態で配信されたとしても、元のコンテンツの真正を保証することが可能となる。

【0176】さらに、コンテンツは、使用条件を有さず、使用条件は、ライセンスに付加されているので、ライセンス内の使用条件を変更することで、それに関係するコンテンツの使用条件を一斉に変更することが可能となる。

【0177】次に、マークの利用方法について説明する。本発明においては、上述したように、使用条件は、コンテンツではなく、ライセンスに付加される。しかしながら、コンテンツによって、使用状況が異なる場合がある。そこで、本発明においては、図25に示されるように、コンテンツにマークが付加される。

【0178】ライセンスとコンテンツは、1対多の関係にあるため、コンテンツの個々の使用状況をライセンスの使用条件にのみ記述するのは困難となる。そこで、このように、コンテンツに使用状況を付加することにより、ライセンスでの管理をしながらも、個々のコンテンツを管理することが可能となる。

【0179】このマークには、例えば、図31に示されるように、ユーザのID(リーフID)、所有権フラグ、使用開始時刻、およびコピー回数等が記述される。

【0180】さらに、マークには、リーフID、所有権フラグ、使用開始時刻、およびコピー回数等のメッセージに基づいて生成されたデジタル署名が付加される。

【0181】所有権フラグは、例えば、所定の期間だけコンテンツを使用可能とするライセンスを、そのまま買い取ったような場合(使用期間を永久に変更したような

場合)に付加される。使用開始時刻は、コンテンツの使用を所定の期間内に開始した場合に記述される。例えば、コンテンツをダウンロードする時期が制限されているような場合において、その期限内にダウンロードが行われたようなとき、その実際にコンテンツをダウンロードした日時がここに記述される。これにより、期間内での有効な使用であることが、証明される。

【0182】コピー回数には、それまでにそのコンテンツをコピーした回数が履歴(ログ)として記述される。

【0183】次に、図32のフローチャートを参照して、ユーザがライセンスを買い取った場合に、マークを付加する処理について、マークをコンテンツに付加する例として説明する。

【0184】最初に、ステップS221において、CPU21は、入力部26からのユーザの指令に基づいて、インターネット2を介して、ライセンスサーバ4にアクセスする。

【0185】ステップS222において、CPU21は、ユーザからの入力部26を介しての入力を取り込み、その入力に対応してライセンスサーバ4に対してライセンスの買い取りを要求する。

【0186】この要求に対応して、図33のフローチャートを参照して後述するように、ライセンスサーバ4は、ライセンスを買い取るために必要な対価を提示してくる(図33のステップS242)。そこで、ステップS223において、クライアント1のCPU21は、ライセンスサーバ4からの対価の提示を受け取ると、これを出力部27に出力し、表示させる。

【0187】ユーザは、この表示に基づいて、提示された対価を了承するか否かを判断し、その判断結果に基づいて、入力部26からその判断結果を入力する。

【0188】CPU21は、ステップS224において、入力部26からの入力に基づいて、ユーザが提示された対価を了承したか否かを判定し、了承したと判定した場合には、ステップS225に進み、ライセンスサーバ4に了承を通知する処理を実行する。

【0189】この了承通知を受信すると、ライセンスサーバ4は、対価の買い取りを表す情報、すなわち所有権フラグを記述したマークを送信してくる(図33のステップS244)。そこで、ステップS226において、クライアント1のCPU21は、ライセンスサーバ4からのマークを受け取ると、ステップS227において、受け取ったマークをコンテンツに埋め込む処理を実行する。すなわち、これにより、買い取られたライセンスに対応するコンテンツのマークとして、図31に示されるような所有権フラグが記述されたマークがコンテンツに対応して記録されることになる。また、このとき、CPU21は、メッセージが更新されたことになるので、デジタル署名(図25)も更新し、記録媒体に記録する。

【0190】ステップS224において、ライセンスサ

ーバ4から提示された対価が了承されていないと判定された場合、ステップS228に進み、CPU21は、提示された対価を了承しないことをライセンスサーバ4に通知する。

【0191】このようなクライアント1の処理に対応して、ライセンスサーバ4は、図33のフローチャートに示す処理を実行する。

【0192】すなわち、最初に、ステップS241において、ライセンスサーバ4のCPU21は、クライアント1からライセンス買い取りの要求が送信されてくると(図32のステップS222)、これを受け取り、ステップS242において、対象とされているライセンスの買い取りに必要な対価を記憶部28から読み出し、これをクライアント1に送信する。

【0193】上述したように、このようにして提示された対価に対して、クライアント1から提示された対価を了承するか否かの通知が送信されてくる。

【0194】そこで、ステップS243において、ライセンスサーバ4のCPU21は、クライアント1から了承通知を受信したか否かを判定し、了承通知を受信したと判定した場合、ステップS244に進み、対象とされるライセンスの買い取りを表すメッセージを含むマークを生成し、自分自身の秘密鍵で、デジタル署名を付加して、クライアント1に送信する。このようにして送信されたマークは、上述したように、クライアント1の記憶部28において、対応するコンテンツに記録される(図32のステップS227)。

【0195】ステップS243において、クライアント1から了承通知が受信されていないと判定された場合、ステップS244の処理はスキップされる。すなわち、この場合には、ライセンスの買い取り処理が最終的に行われなかったことになるので、マークは送信されない。

【0196】図34は、ステップS244において、ライセンスサーバ4からクライアント1に対して送信されるマークの構成例を表している。この例においては、そのユーザのリーフID、所有権フラグ(Own)、並びにリーフIDと所有権フラグを、ライセンスサーバ4の秘密鍵Sに基づいて生成されたデジタル署名Sig_S(LeafID, Own)により、マークが構成されている。

【0197】なお、このマークは、特定のユーザの特定のコンテンツに対してのみ有効なものであるため、対象とされるコンテンツがコピーされた場合には、そのコピーされたコンテンツに付随するマークは無効とされる。

【0198】このようにして、コンテンツとライセンスを分離し、使用条件をライセンスに対応させる場合においても、個々のコンテンツの使用状況に応じたサービスを実現することが可能となる。

【0199】次に、グルーピングについて説明する。複数の機器やメディアを適当に集め、その1つの集合内においては、コンテンツを自由に授受することができるよ

うにすることは、グルーピングと称される。通常、このグルーピングは、個人の所有する機器やメディアにおいて行われる。このグルーピングは、従来、グループ毎にグループキーを設定する等して行われていたが、グループ化する複数の機器やメディアに、同一のライセンスを対応づけることにより、容易にグルーピングすることが可能となる。

【0200】また、各機器を予め登録しておくことで、グルーピングすることも可能である。この場合のグルーピングについて、以下に説明する。

【0201】この場合、ユーザは、グルーピング対象とされる機器の証明書を予めサーバに登録しておく必要がある。この証明書の登録処理について、図35と図36のフローチャートを参照して説明する。

【0202】最初に、図35のフローチャートを参照して、クライアント（グルーピング対象となる機器）の証明書の登録処理について説明する。ステップS261において、クライアント1のCPU21は、グルーピングの対象とされる機器としての自分自身の証明書を作成する。この証明書には、自分自身の公開鍵が含まれる。

【0203】次に、ステップS262に進み、CPU21は、ユーザの入力部26からの入力に基づいて、コンテンツサーバ3にアクセスし、ステップS263において、ステップS261の処理で作成された証明書をコンテンツサーバ3に送信する処理を実行する。

【0204】なお、証明書としては、ライセンスサーバ4から受信したものを、そのまま使用することもできる。

【0205】以上の処理は、グルーピング対象とされる全ての機器が行う。

【0206】次に、図36のフローチャートを参照して、図35のクライアント1の証明書の登録処理に対応して行われるコンテンツサーバ3の証明書の登録処理について説明する。

【0207】最初に、ステップS271において、コンテンツサーバ3のCPU21は、クライアント1から送信されてきた証明書を受信すると、ステップS272において、その証明書を記憶部28に登録する。

【0208】以上の処理が、グループ対象とされる機器毎に行われる。その結果、コンテンツサーバ3の記憶部28には、例えば、図37に示されるように、グループ毎に、そのグループを構成するデバイスの証明書が登録される。

【0209】図37に示される例では、グループ1の証明書として、証明書C11乃至C14が登録されている。これらの証明書C11乃至C14には、対応する公開鍵Kp11乃至Kp14が含まれている。

【0210】同様に、グループ2の証明書として、証明書C21乃至C23が登録されており、これらに対応する公開鍵Kp21乃至Kp23が含まれている。

【0211】以上のようなグループを構成する各機器毎に、その証明書が登録された状態において、ユーザからそのグループに属する機器にコンテンツの提供が要求されると、コンテンツサーバ3は、図38のフローチャートに示す処理を実行する。

【0212】最初に、ステップS281において、コンテンツサーバ3のCPU21は、記憶部28に記憶されている証明書のうち、そのグループに属する証明書を検証する処理を実行する。

【0213】この検証処理は、図29と図30を参照して説明されたように、各機器の証明書に含まれるリーフIDに基づいて、タグを利用してEKBをたどることで行われる。EKBは、コンテンツサーバ3にも、ライセンスサーバ4から配布されている。この検証処理により、リボークされている証明書は除外される。

【0214】ステップS282において、コンテンツサーバ3のCPU21は、ステップS281の検証処理の結果、有効とされた証明書を選択する。そして、ステップS283において、CPU21は、ステップS282の処理で選択された各機器の証明書の各公開鍵でコンテンツ鍵を暗号化する。ステップS284において、CPU21は、対象とされるグループの各機器に、ステップS283の処理で暗号化されたコンテンツ鍵をコンテンツとともに送信する。

【0215】図37に示されるグループ1のうち、例えば、証明書C14がリボークされているとすると、ステップS283の処理で、例えば、図39に示されるような暗号化データが生成される。

【0216】すなわち、図39の例においては、コンテンツ鍵Kcが、証明書C11の公開鍵Kp11、証明書C12の公開鍵Kp12、または証明書C13の公開鍵Kp13により、暗号化されている。

【0217】コンテンツサーバ3の図38に示されるような処理に対応して、コンテンツの提供を受ける各グループの機器（クライアント）は、図40のフローチャートに示す処理を実行する。

【0218】最初に、ステップS291において、クライアント1のCPU21は、コンテンツサーバ3が図38のステップS284の処理で送信してきたコンテンツを、コンテンツ鍵とともに受信する。コンテンツは、コンテンツ鍵Kcにより、暗号化されており、コンテンツ鍵は上述したように、各機器が保持する公開鍵により暗号化されている（図39）。

【0219】そこで、ステップS292において、CPU21は、ステップS291の処理で受信した自分宛のコンテンツ鍵を、自分自身の秘密鍵で復号し、取得する。そして、取得したコンテンツ鍵を用いてコンテンツの復号処理が行われる。

【0220】例えば、図39の例に示される証明書C11に対応する機器は、公開鍵Kp11に対応する自分自身

の秘密鍵を用いて、コンテンツ鍵Kcの暗号を復号し、コンテンツ鍵Kcを取得する。そして、コンテンツ鍵Kcを用いて、コンテンツがさらに復号される。

【0221】同様の処理は、証明書C12、C13に対応する機器においても行われる。リボークされている証明書C14の機器は、自分自身の公開鍵を用いて暗号化されたコンテンツ鍵Kcがコンテンツに付随して送られてこないで、コンテンツ鍵Kcを復号することができず、従って、コンテンツ鍵Kcを用いてコンテンツを復号することができない。

【0222】以上においては、コンテンツキー（すなわちコンテンツ）に対してグルーピングを行うようにしたが、ライセンスキー（ライセンス）に対してグルーピングを行うことも可能である。

【0223】以上のようにして、特別なグループキーや、後述するICV（Integrity Check Value）を用いずにグループ化が可能となる。このグループ化は、小規模のグループに適用するのに向いている。

【0224】本発明においては、ライセンスもチェックアウト、あるいはチェックインしたり、ムーブしたり、コピーしたりすることが可能とされる。但し、これらの処理はSDMIで定められたルールに基づいて行われる。

【0225】次に、図41と図42のフローチャートを参照して、このようなクライアントによるライセンスのチェックアウト処理について説明する。

【0226】最初に、図41のフローチャートを参照して他のクライアントにライセンスをチェックアウトするクライアントの処理について説明する。最初に、ステップS301において、クライアント1のCPU21は、チェックアウト対象のライセンスのチェックアウト回数N1を読み取る。このチェックアウト回数は、図8に示される使用条件に書き込まれているので、この使用条件から読み取られる。

【0227】次に、ステップS302において、CPU21は、チェックアウト対象のライセンスの最大チェックアウト回数N2を、やはりライセンスの使用条件から読み取る。

【0228】そして、ステップS303において、CPU21は、ステップS301の処理で読み取られたチェックアウト回数N1と、ステップS302の処理で読み取られた最大チェックアウト回数N2とを比較し、チェックアウト回数N1が最大チェックアウト回数N2より大きいかなかを判定する。

【0229】チェックアウト回数N1が、最大チェックアウト回数N2より小さいと判定された場合、ステップS304に進み、CPU21は、相手側の装置（チェックアウト先のクライアント）のリーフキーを相手個々の装置から取得し、そのリーフキーを、いまチェックアウト対象とされているライセンスIDに対応して記憶部28のチェックアウトリストに記憶させる。

【0230】次に、ステップS305において、CPU21は、ステップS301の処理で読み取られたライセンスのチェックアウト回数N1の値を1だけインクリメントする。ステップS306において、CPU21は、ライセンスのメッセージに基づいて、ICVを演算する。このICVについては、図46乃至図50を参照して後述する。ICVを用いてライセンスの改竄を防止することが可能となる。

【0231】次に、ステップS307において、CPU21は、チェックアウト対象のライセンスと、ステップS306の処理で演算されたICVを、自分自身の公開鍵を用いて暗号化して、EKBおよび証明書とともに、相手側の装置に出力し、コピーさせる。さらに、ステップS308において、CPU21は、ステップS306の処理で演算されたICVを、相手側装置のリーフキーと、ライセンスIDに対応して記憶部28のチェックリスト中に記憶させる。

【0232】ステップS303において、チェックアウト回数N1が最大チェックアウト回数N2より小さくない（例えば、等しい）と判定された場合、もはや許容される回数だけチェックアウトが行われているので、これ以上チェックアウトを行うことができない。そこで、ステップS309に進み、CPU21は、エラー処理を実行する。すなわち、この場合、チェックアウト処理は実行されないことになる。

【0233】次に、図42のフローチャートを参照して、図41のチェックアウト処理により、ライセンスのチェックアウトを受けるクライアントの処理について説明する。

【0234】最初に、ステップS321において、相手側装置（ライセンスをチェックアウトするクライアント1）に、自分自身のリーフキーを送信する。このリーフキーは、ステップS304において、相手側のクライアントにより、ライセンスIDに対応して記憶される。

【0235】次に、ステップS322において、CPU21は、相手側のクライアント1から暗号化されたライセンスとICVが、EKBおよび証明書とともに送信されてきた場合、これを受信する。すなわち、このライセンス、ICV、EKBおよび証明書は、図41のステップS307の処理で相手側の装置から送信されたものである。

【0236】ステップS323において、CPU21は、ステップS322の処理で受信したライセンス、ICV、EKBおよび証明書を、記憶部28に記憶させる。

【0237】以上のようにして、ライセンスのチェックアウトを受けたクライアント1は、チェックアウトを受けたそのライセンスを使用して、所定のコンテンツを再生する場合、図43のフローチャートに示される処理を実行する。

【0238】すなわち、最初に、ステップS341において、クライアント1のCPU21は、ユーザより入力部

26を介して再生が指定されたコンテンツのICVを演算する。そして、ステップS342において、CPU21は、記憶部28に記憶されている暗号化されているICVを、証明書に含まれている公開鍵に基づいて、復号させる。

【0239】次に、ステップS343において、CPU21は、ステップS341の処理により、いま演算されたICVと、ステップS342の処理により読み出され、復号されたICVが一致するかどうかを判定する。両者が一致する場合には、ライセンスは改竄されていないことになる。そこで、ステップS344にすすみ、CPU21は、対応するコンテンツを再生する処理を実行する。

【0240】これに対して、ステップS343において、2つのICVが一致しないと判定された場合、ライセンスは改竄されている恐れがある。このため、ステップS345に進み、CPU21は、エラー処理を実行する。すなわち、このとき、そのライセンスを用いてコンテンツを再生することができないことになる。

【0241】次に、以上のようにして、他のクライアントに一旦チェックアウトしたライセンスのチェックインを受けるクライアントの処理について、図44のフローチャートを参照して説明する。

【0242】最初に、ステップS361において、CPU21は、相手側の装置（ライセンスを返却（チェックイン）してくるクライアント1）のリーフキーと、チェックイン対象のライセンスのIDを取得する。次に、ステップS362において、CPU21は、ステップS361で取得されたチェックイン対象のライセンスが、自分自身が相手側装置にチェックアウトしたライセンスであるかどうかを判定する。この判定は、図41のステップS308の処理で記憶されたICV、リーフキー、およびライセンスIDに基づいて行われる。すなわち、ステップS361で取得されたリーフキー、ライセンスID、およびICVが、チェックアウトリスト中に記憶されているかが判定され、記憶されている場合には、自分自身がチェックアウトしたライセンスであると判定される。

【0243】ライセンスが、自分自身がチェックアウトしたものであるとき、ステップS363において、CPU21は、相手側の装置のライセンス、EKBおよび証明書の削除を要求する。後述するように、この要求に基づいて、相手側の装置は、ライセンス、EKBおよび証明書の削除を実行する（図45のステップS383）。

【0244】ステップS364において、CPU21は、一旦チェックアウトしたライセンスが再びチェックインされてきたので、そのライセンスのチェックアウト回数N1を1だけデクリメントする。

【0245】ステップS365において、CPU21は、相手側の装置に他のライセンスをチェックアウトしているかどうかを判定し、まだチェックアウトしている他のライセンスが存在しない場合には、ステップS366に進

み、CPU21は、相手側の装置のチェックイン対象機器としてのチェックアウトリストにおける記憶を削除する。これに対して、ステップS365において、相手側の装置にチェックアウトしている他のライセンスが存在すると判定された場合には、他のライセンスのチェックインを受ける可能性があるので、ステップS366の処理はスキップされる。

【0246】ステップS362において、チェックイン対象とされているライセンスが、自分自身が相手側装置にチェックアウトしたライセンスではないと判定された場合、CPU21は、ステップS367に進み、エラー処理を実行する。すなわち、この場合には、自分自身が管轄するライセンスではないことになるので、チェックイン処理は実行されない。

【0247】ユーザが、ライセンスを不正にコピーしたような場合、記憶されているICVの値と、ステップS361の処理で取得されたライセンスに基づいて演算されたICVの値が異なるものとなるので、チェックインできないことになる。

【0248】図45は、図44のフローチャートに示されるライセンスのチェックイン処理を実行するクライアントに対して、自分自身が有しているライセンスをチェックインさせるクライアントの処理を表している。

【0249】ステップS381において、クライアント1のCPU21は、相手側の装置（図44のフローチャートに示す処理を実行するクライアント1）にリーフキーとチェックイン対象のライセンスのIDを送信する。上述したように、相手側の装置は、ステップS361において、このリーフキーとライセンスIDを取得し、ステップS362において、それに基づいて、チェックイン対象のライセンスの認証処理を実行する。

【0250】ステップS382において、クライアント1のCPU21は、相手側の装置からライセンスの削除を要求されたかどうかを判定する。すなわち、ライセンスが正当なチェックイン対象のライセンスである場合、上述したように、相手側の装置は、ステップS363の処理でライセンス、EKBおよび証明書の削除を要求してくる。そこで、この要求を受信した場合、ステップS383に進み、CPU21は、ライセンス、EKBおよび証明書を削除する。すなわち、これにより、このクライアント1は、以後そのライセンスを使用できない状態となり、図44のステップS364の処理により、チェックアウト回数N1が、1だけデクリメントされるので、チェックインが完了したことになる。

【0251】ステップS382において、相手側の装置からライセンスの削除が要求されていないと判定された場合、ステップS384に進み、エラー処理が実行される。すなわち、この場合には、ICVの値が異なっている等の理由により、チェックインができないことになる。

【0252】以上においては、チェックインとチェック

アウトについて説明したが、同様に、ライセンスをコピーあるいはムーブさせるようにすることも可能である。

【0253】次に、ライセンス（コンテンツも同様）の改竄を防止するためにライセンスのインテグリティ・チェック値（ICV）を生成して、ライセンスに対応付けて、ICVの計算により、ライセンス改竄の有無を判定する処理構成について説明する。

【0254】ライセンスのインテグリティ・チェック値（ICV）は、例えばライセンスに対するハッシュ関数を用いて計算され、 $ICV = hash(Kicv, L1, L2, \dots)$ によって計算される。KicvはICV生成キーである。L1, L2はライセンスの情報であり、ライセンスの重要情報のメッセージ認証符号（MAC: Message authentication Code）が使用される。

【0255】DES暗号処理構成を用いたMAC値生成例を図46に示す。図46の構成に示すように対象となるメッセージを8バイト単位に分割し、（以下、分割されたメッセージをM1、M2、・・・、MNとする）、まず、初期値（IV）とM1を、演算部24-1Aにより排他的論理和する（その結果をI1とする）。次に、I1をDES暗号化部24-1Bに入れ、鍵（以下、K1とする）を用いて暗号化する（出力をE1とする）。続けて、E1およびM2を演算部24-2Aにより排他的論理和し、その出力I2をDES暗号化部24-2Bへ入れ、鍵K1を用いて暗号化する（出力E2）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。DES暗号化部24-NBから最後に出てきたENがメッセージ認証符号（MAC（Message Authentication Code））となる。

【0256】このようなライセンスのMAC値とICV生成キーにハッシュ関数を適用してライセンスのインテグリティ・チェック値（ICV）が生成される。例えばライセンス生成時に生成したICVと、新たにライセンスに基づいて生成したICVとを比較して同一のICVが得られればライセンスに改竄のないことが保証され、ICVが異なれば、改竄があったと判定される。

【0257】次に、ライセンスのインテグリティ・チェック値（ICV）生成キーであるKicvを上述の有効化キープブロックによって送付する構成について説明する。すなわちEKBによる暗号化メッセージデータをライセンスのインテグリティ・チェック値（ICV）生成キーとした例である。

【0258】図47および図48に複数のデバイスに共通のライセンスを送付した場合、それらのライセンスの改竄の有無を検証するためのインテグリティ・チェック値生成キーKicvを有効化キープブロック（EKB）によって配信する構成例を示す。図47はデバイス0, 1, 2, 3に対して復号可能なチェック値生成キーKicvを配信する例を示し、図48はデバイス0, 1, 2, 3中のデバイス3をリボーク（排除）してデバイス

0, 1, 2に対してのみ復号可能なチェック値生成キーKicvを配信する例を示す。

【0259】図47の例では、更新ノードキーK(t)00によって、チェック値生成キーKicvを暗号化したデータEnc(K(t)00, Kicv)とともに、デバイス0, 1, 2, 3においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキーK(t)00を復号可能な有効化キープブロック（EKB）を生成して配信する。それぞれのデバイスは、図47の右側に示すように、まず、EKBを処理（復号）することにより、更新されたノードキーK(t)00を取得し、次に、取得したノードキーK(t)00を用いて、暗号化されたチェック値生成キーEnc(K(t)00, Kicv)を復号して、チェック値生成キーKicvを得ることが可能となる。

【0260】その他のデバイス4, 5, 6, 7・・・は同一の有効化キープブロック（EKB）を受信しても自身の保有するノードキー、リーフキーでは、EKBを処理して更新されたノードキーK(t)00を取得することができないので、安全に正当なデバイスに対してのみチェック値生成キーを送付することができる。

【0261】一方、図48の例は、図12の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス0, 1, 2, に対してのみ復号可能な有効化キープブロック（EKB）を生成して配信した例である。図48に示す有効化キープブロック（EKB）と、チェック値生成キー（Kicv）をノードキー（K(t)00）で暗号化したデータEnc(K(t)00, Kicv)を配信する。

【0262】図48の右側には、復号手順を示してある。デバイス0, 1, 2は、まず、受領した有効化キープブロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー（K(t)00）を取得する。次に、K(t)00による復号によりチェック値生成キーKicvを取得する。

【0263】図12に示す他のグループのデバイス4, 5, 6・・・は、この同様のデータ（EKB）を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー（K(t)00）を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー（K(t)00）を取得することができず、正当な権利を有するデバイスのみがチェック値生成キーを復号して利用することが可能となる。

【0264】このように、EKBを利用したチェック値生成キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能としたチェック値生成キーを配信することが可能となる。

【0265】このようなライセンスのインテグリティ・

チェック値（ICV）を用いることにより、EKBと暗号化ライセンスの不正コピーを排除することができる。例えば図49Aに示すように、ライセンスL1とライセンスL2とをそれぞれのライセンスキーを取得可能な有効化キーブロック（EKB）とともに格納したメディア1があり、これをそのままメディア2にコピーした場合を想定する。EKBと暗号化ライセンスのコピーは可能であり、これをEKBを復号可能なデバイスでは利用できることになる。

【0266】図49Bに示す例では、各メディアに正当に格納されたライセンスに対応付けてインテグリティ・チェック値（ICV（L1，L2））を格納する構成とする。なお、（ICV（L1，L2））は、ライセンスL1とライセンスL2にハッシュ関数を用いて計算されるライセンスのインテグリティ・チェック値である $ICV = hash(Kicv, L1, L2)$ を示している。図49Bの構成において、メディア1には正当にライセンス1とライセンス2が格納され、ライセンスL1とライセンスL2に基づいて生成されたインテグリティ・チェック値（ICV（L1，L2））が格納される。また、メディア2には正当にライセンス1が格納され、ライセンスL1に基づいて生成されたインテグリティ・チェック値（ICV（L1））が格納される。

【0267】この構成において、メディア1に格納された{EKB，ライセンス2}をメディア2にコピーしたとすると、メディア2で、ライセンスチェック値を新たに生成すると、ICV（L1，L2）が生成されることになり、メディア2に格納されているKicv（L1）と異なり、ライセンスの改竄あるいは不正なコピーによる新たなライセンスの格納が実行されたことが明らかになる。メディアを再生するデバイスにおいて、再生ステップの前ステップにICVチェックを実行して、生成ICVと格納ICVの一致を判別し、一致しない場合は、再生を実行しない構成とすることにより、不正コピーのライセンスの再生を防止することが可能となる。

【0268】また、さらに、安全性を高めるため、ライセンスのインテグリティ・チェック値（ICV）を書き換えカウンタを含めたデータに基づいて生成する構成としてもよい。すなわち $ICV = hash(Kicv, counter+1, L1, L2, \dots)$ によって計算する構成とする。ここで、カウンタ（counter+1）は、ICVの書き換えごとに1つインクリメントされる値として設定する。なお、カウンタ値はセキュアなメモリに格納する構成とすることが必要である。

【0269】さらに、ライセンスのインテグリティ・チェック値（ICV）をライセンスと同一メディアに格納することができない構成においては、ライセンスのインテグリティ・チェック値（ICV）をライセンスとは別のメディア上に格納する構成としてもよい。

【0270】例えば、読み込み専用メディアや通常のM

O等のコピー防止策のとられていないメディアにライセンスを格納する場合、同一メディアにインテグリティ・チェック値（ICV）を格納するとICVの書き換えが不正なユーザによりなされる可能性があり、ICVの安全性が保てないおそれがある。この様な場合、ホストマシン上の安全なメディアにICVを格納して、ライセンスのコピーコントロール（例えばcheck-in/check-out、move）にICVを使用する構成とすることにより、ICVの安全な管理およびライセンスの改竄チェックが可能となる。

【0271】この構成例を図50に示す。図50では読み込み専用メディアや通常のMO等のコピー防止策のとられていないメディア2201にライセンス1乃至ライセンス3が格納され、これらのライセンスに関するインテグリティ・チェック値（ICV）を、ユーザが自由にアクセスすることの許可されないホストマシン上の安全なメディア2202に格納し、ユーザによる不正なインテグリティ・チェック値（ICV）の書き換えを防止した例である。このような構成として、例えばメディア2201を装着したデバイスが、メディア2201の再生を実行する際にホストマシンであるPC、サーバにおいてICVのチェックを実行して再生の可否を判定する構成とすれば、不正なコピーライセンスあるいは改竄ライセンスの再生を防止できる。

【0272】本発明が適用されるクライアントは、いわゆるパーソナルコンピュータ以外に、PDA（Personal Digital Assistants）、携帯電話機、ゲーム端末機などとしてすることができる。

【0273】一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【0274】この記録媒体は、図2に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク41（フロッピディスクを含む）、光ディスク42

（CD-ROM（Compact Disk - Read Only Memory）、DVD（Digital Versatile Disk）を含む）、光磁気ディスク43（MD（Mini-Disk）を含む）、もしくは半導体メモリ44などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM22や、記憶部28に含まれるハードディスクなどで構成される。

【0275】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に

実行される処理をも含むものである。

【0276】また、セキュリティに関連する処理を実行させるプログラムは、その処理を解析されるのを防ぐため、そのプログラム自体が暗号化されているのが望ましい。例えば、暗号処理などを行う処理については、そのプログラムをタンパーレジスタントモジュールとして構成することができる。

【0277】また、コンテンツを利用許可するライセンスを特定するためにコンテンツのヘッダに記載されている情報はライセンスを一意に識別するライセンスIDでなくてもよい。上記の実施例では、ライセンスIDが、コンテンツの利用に必要なライセンスを特定する情報であり、あるライセンスが利用を許可するコンテンツを特定する情報であり、クライアント1からライセンス要求によって要求されるライセンスを識別する情報である。コンテンツにコンテンツのそのコンテンツに関する各種属性情報のリストが記載され、ライセンスに、そのライセンスによって利用許可されるコンテンツの条件式を記載するようにしても良い。この場合では、コンテンツに含まれる属性情報がそのコンテンツの利用を許可するライセンスを特定する情報であり、ライセンスに含まれる条件式がそのライセンスが利用を許可するコンテンツを特定する情報であり、ライセンスIDはライセンスを一意に識別する情報となる。このようにした場合には、一つのコンテンツに複数のライセンスを対応付けることが可能になり、ライセンスの発行を柔軟に行うことができる。

【0278】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0279】

【発明の効果】以上の如く、本発明の情報処理装置および方法、ライセンスサーバ、並びにプログラムによれば、暗号化されたデータを自由に配布できるようにし、別途ライセンスを取得することでコンテンツを利用できるようにしたことで、コンテンツの流通を妨げることなく、著作権を保護し、適切な使用料の徴収をすることができる。

【図面の簡単な説明】

【図1】本発明を適用したコンテンツ提供システムの構成を示すブロック図である。

【図2】図1のクライアントの構成を示すブロック図である。

【図3】図1のクライアントのコンテンツのダウンロード処理を説明するフローチャートである。

【図4】図1のコンテンツサーバのコンテンツ提供処理を説明するフローチャートである。

【図5】図4のステップS26におけるフォーマットの例を示す図である。

【図6】図1のクライアントのコンテンツ再生処理を説

明するフローチャートである。

【図7】図6のステップS43のライセンス取得処理の詳細を説明するフローチャートである。

【図8】ライセンスの構成を示す図である。

【図9】図1のライセンスサーバのライセンス提供の処理を説明するフローチャートである。

【図10】図6のステップS45におけるライセンス更新処理の詳細を説明するフローチャートである。

【図11】図1のライセンスサーバのライセンス更新処理を説明するフローチャートである。

【図12】キーの構成を説明する図である。

【図13】カテゴリノードを説明する図である。

【図14】ノードとデバイスの対応の具体例を示す図である。

【図15】有効化キープブロックの構成を説明する図である。

【図16】有効化キープブロックの利用を説明する図である。

【図17】有効化キープブロックのフォーマットの例を示す図である。

【図18】有効化キープブロックのタグの構成を説明する図である。

【図19】DNKを用いたコンテンツの復号処理を説明する図である。

【図20】有効化キープブロックの例を示す図である。

【図21】複数のコンテンツの1つのデバイスに対する割り当てを説明する図である。

【図22】ライセンスのカテゴリを説明する図である。

【図23】クライアントのリッピング処理を説明するフローチャートである。

【図24】ウォーターマークの構成を説明する図である。

【図25】コンテンツのフォーマットの例を示す図である。

【図26】公開鍵証明書の例を示す図である。

【図27】コンテンツの配布を説明する図である。

【図28】クライアントのコンテンツのチェックアウト処理を説明するフローチャートである。

【図29】タグによる有効化キープブロックをたどる例を説明する図である。

【図30】有効化キープブロックの構成例を示す図である。

【図31】マークの構成を説明する図である。

【図32】クライアントのライセンス買い取り処理を説明するフローチャートである。

【図33】ライセンスサーバのライセンス買い取り処理を説明するフローチャートである。

【図34】マークの構成例を示す図である。

【図35】クライアントの証明書の登録処理を説明するフローチャートである。

【図36】コンテンツサーバの証明書登録処理を説明するフローチャートである。

【図37】グループの証明書の例を示す図である。

【図38】グルーピングが行われている場合におけるコンテンツサーバの処理を説明するフローチャートである。

【図39】コンテンツキーの暗号化の例を示す図である。

【図40】グループに属するクライアントの処理を説明するフローチャートである。

【図41】他のクライアントにライセンスをチェックアウトするクライアントの処理を説明するフローチャートである。

【図42】他のクライアントからライセンスのチェックアウトを受けるクライアントの処理を説明するフローチャートである。

【図43】ライセンスのチェックアウトを受けたクライアントの再生処理を説明するフローチャートである。

【図44】他のクライアントからライセンスのチェックインを受けるクライアントの処理を説明するフローチャートである。

ートである。

【図45】他のクライアントにライセンスをチェックインするクライアントの処理を説明するフローチャートである。

【図46】MACの生成を説明する図である。

【図47】ICV生成キーの復号処理を説明するフローチャートである。

【図48】ICV生成キーの他の復号処理を説明する図である。

【図49】ICVによるライセンスのコピーの管理を説明する図である。

【図50】ライセンスの管理を説明する図である。

【符号の説明】

1-1, 1-2 クライアント, 2 インターネット, 3 コンテンツサーバ, 4 ライセンスサーバ, 5 課金サーバ, 20 タイマ, 21 CPU, 24 暗号化復号部, 25 コーデック部, 26 入力部, 27 出力部, 28 記憶部, 29 通信部

【図1】

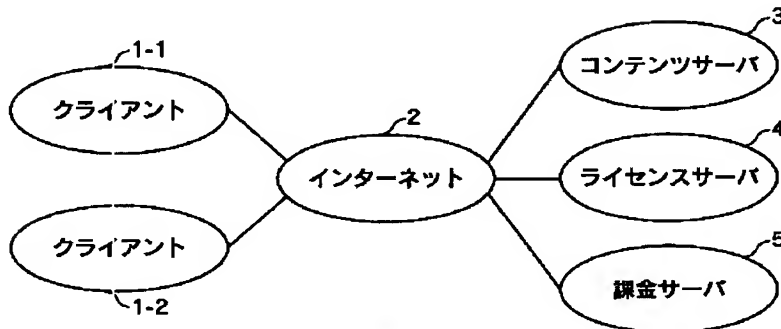


図1

【図3】

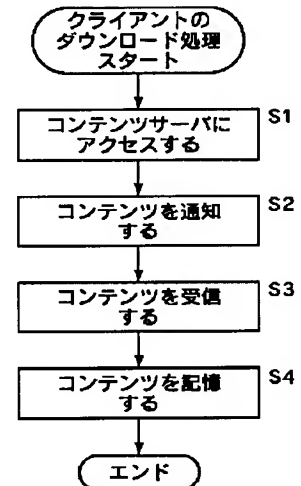


図3

【図8】

	ライセンスID
	作成日時
	有効期限
	使用条件
	リーフID
	電子署名

ライセンス

図8

【図20】

EKB

Enc(DNK, KR)

図20

【図2】

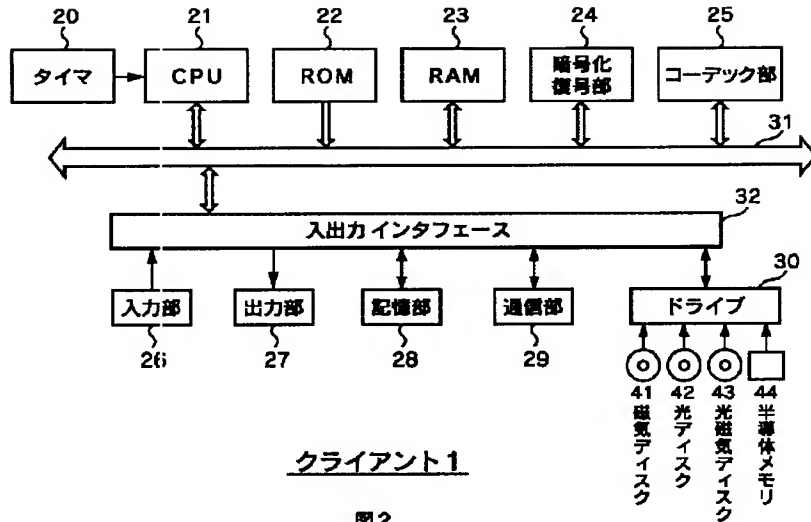


図2

【図4】

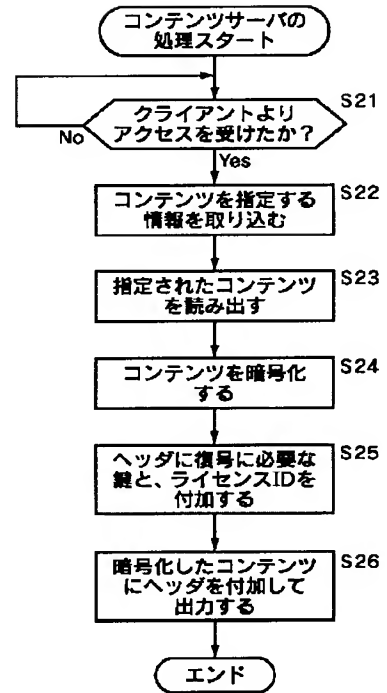


図4

【図5】

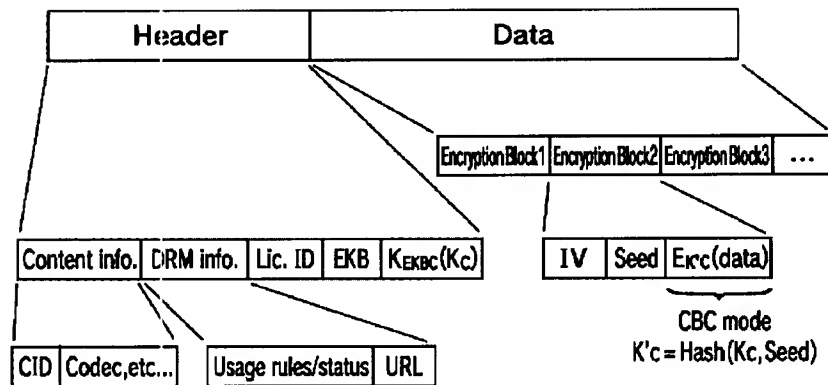


図5

【図11】

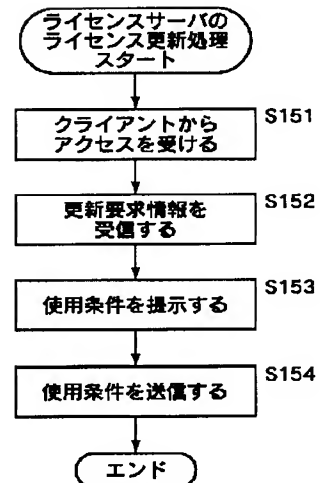


図11

【図6】

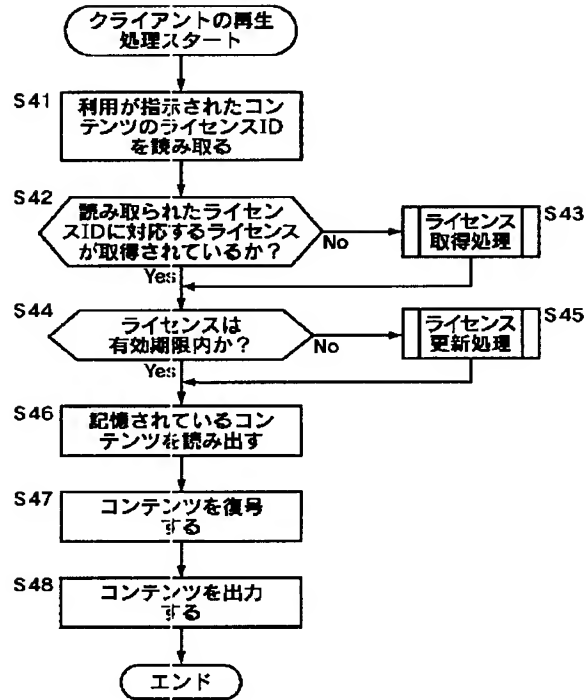


図6

【図7】

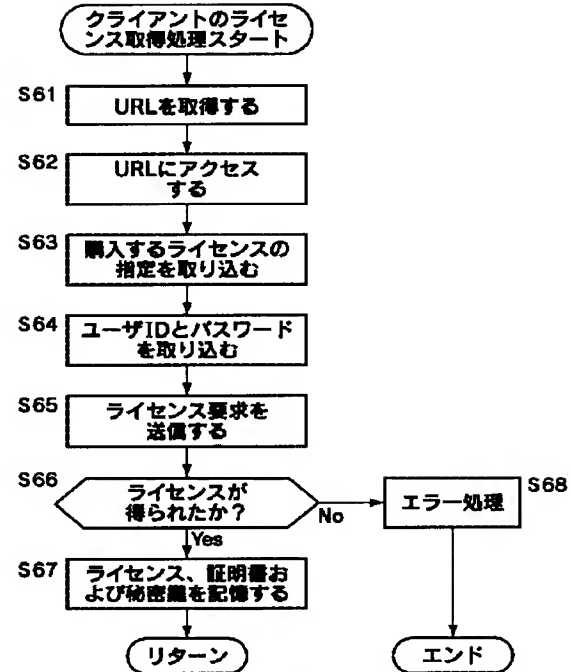


図7

【図12】

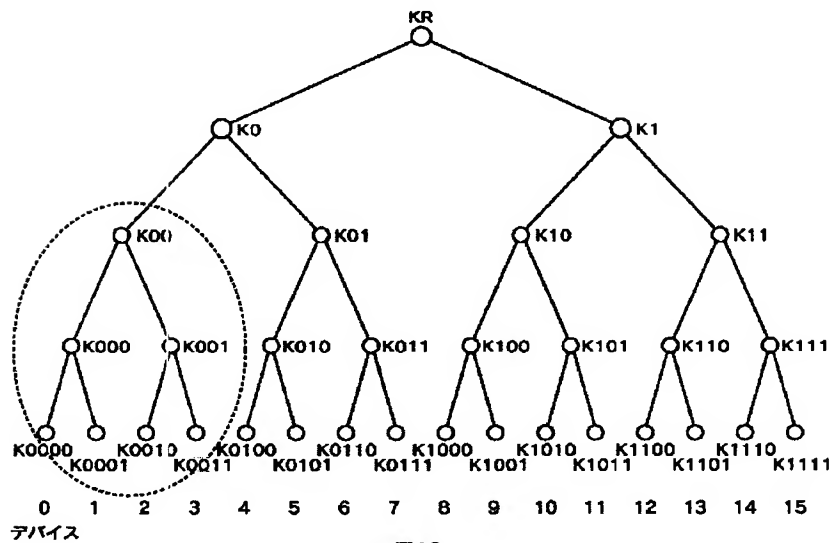


図12

【図23】

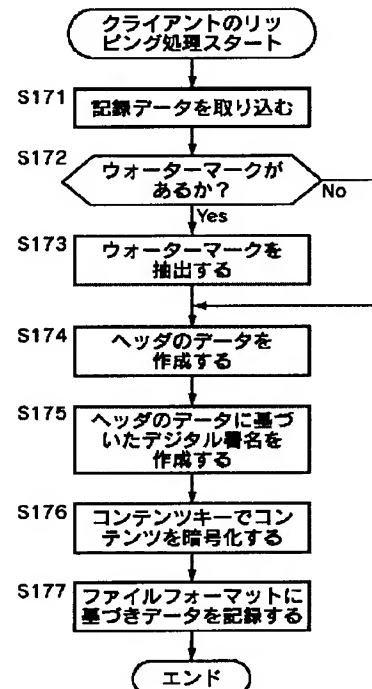
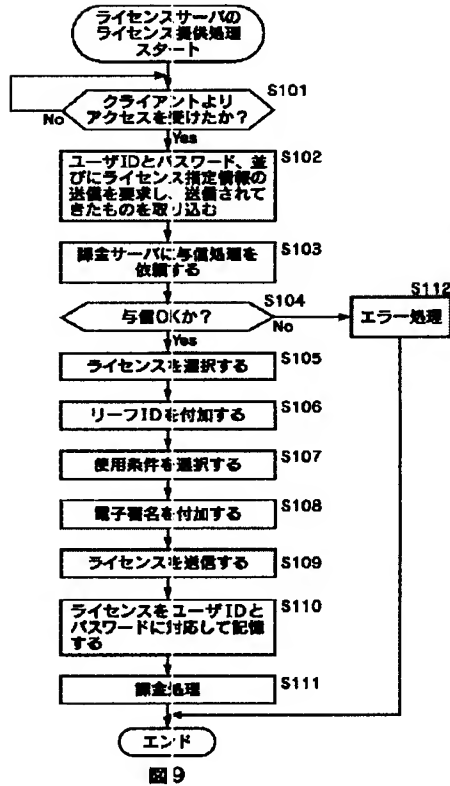
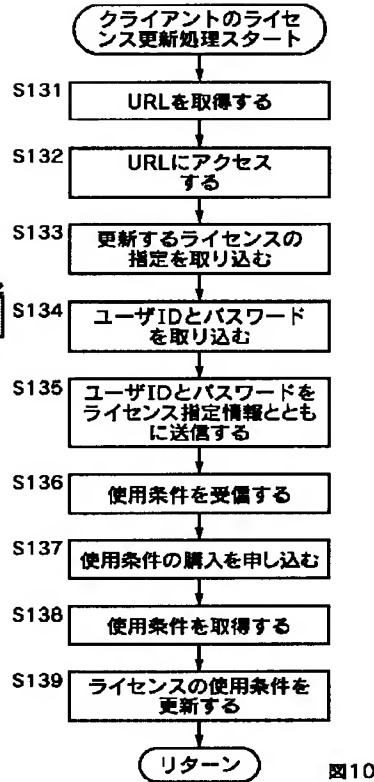


図23

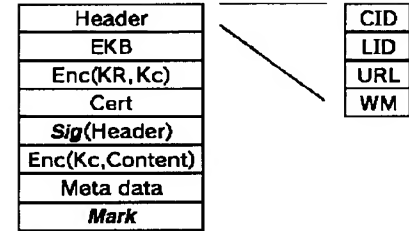
【図9】



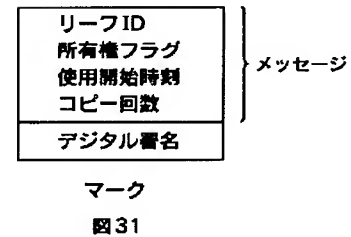
【図10】



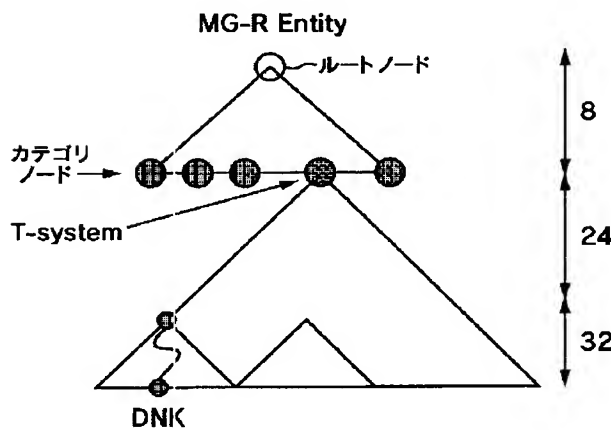
【図25】



【図31】



【図13】



【図34】

Mark = { LeafID, Own, Sig_S(LeafID, Own)}

図34

【図15】

A 有効化キーブロック(EKB:Enabling Key Block)
デバイス0,1,2にバージョン:tのノードキーを送付

バージョン (Version) : t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

B 有効化キーブロック(EKB:Enabling Key Block)
デバイス0,1,2にバージョン:tのノードキーを送付

バージョン (Version) : t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

図15

【図14】

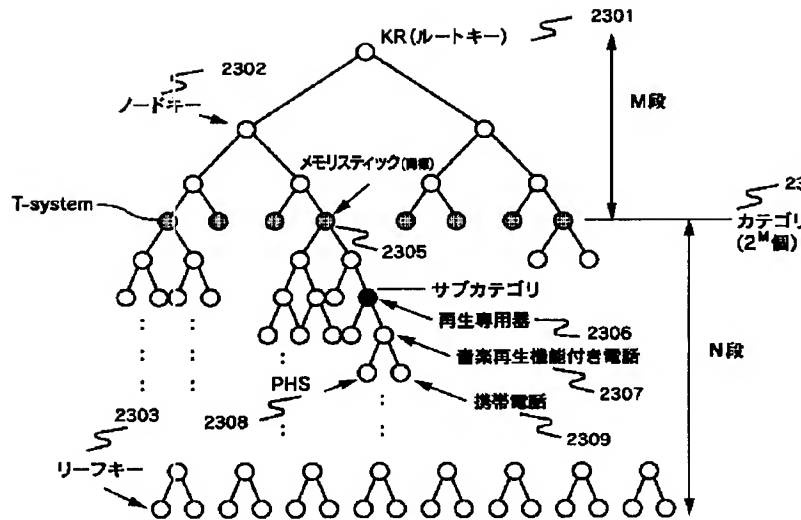


図14

【図16】

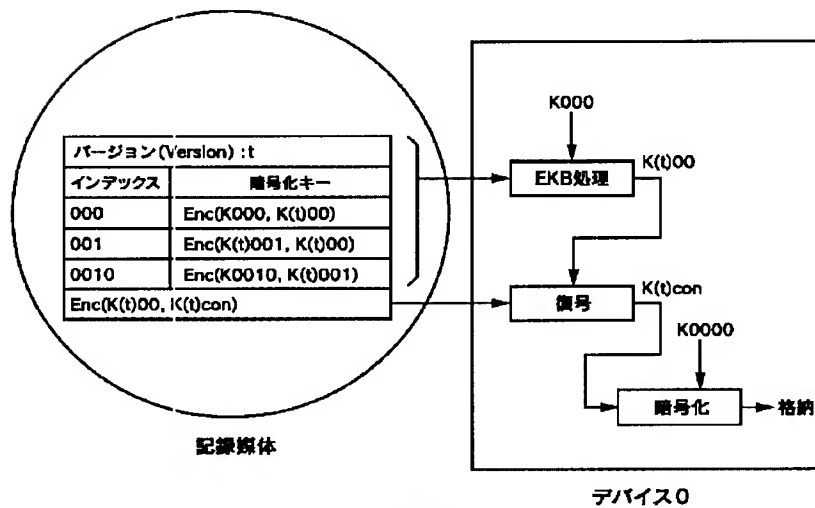


図16

【図39】

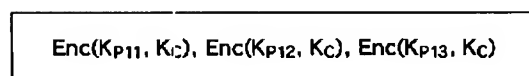


図39

【図33】

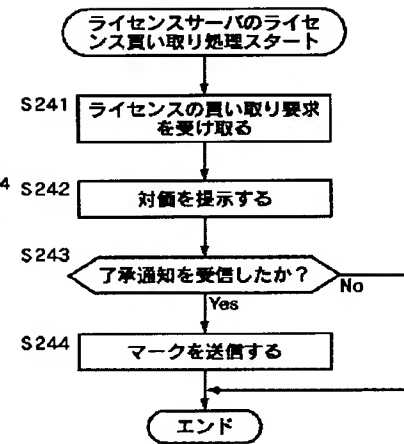


図33

【図35】

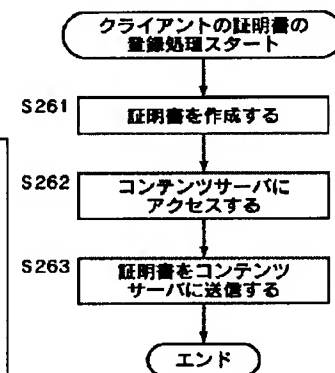


図35

【図36】

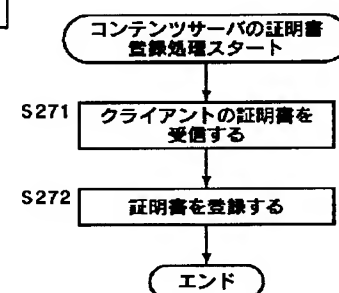


図36

【図17】

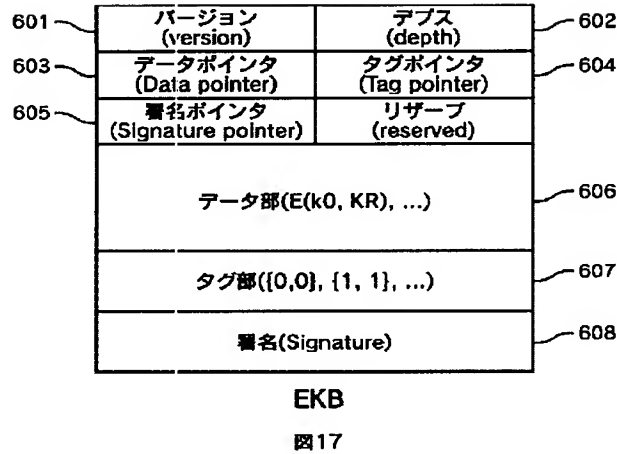


図17

【図18】

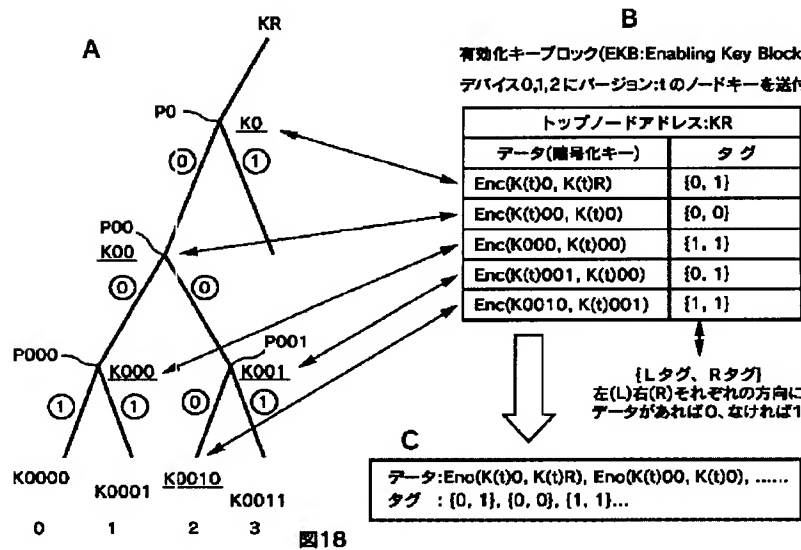


図18

【図37】

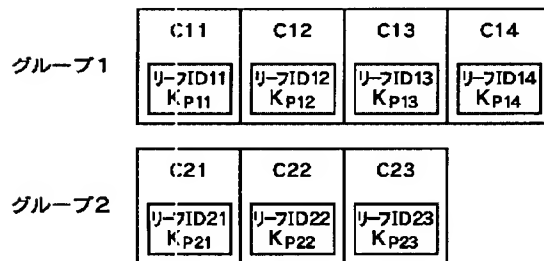


図37

【図40】

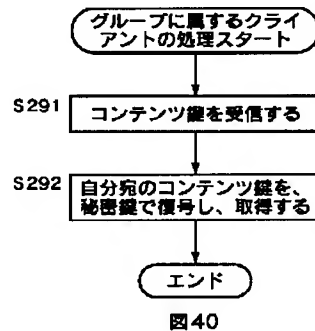


図40

【図19】

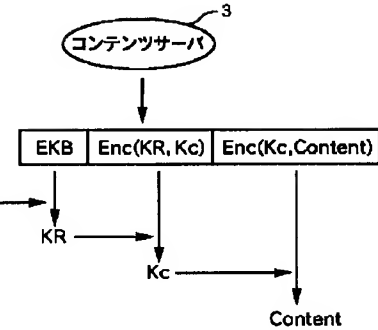


図19

【図38】

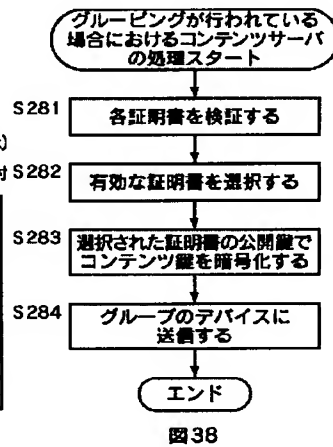


図38

【図42】

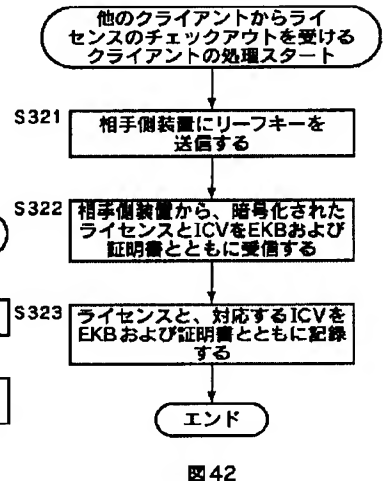
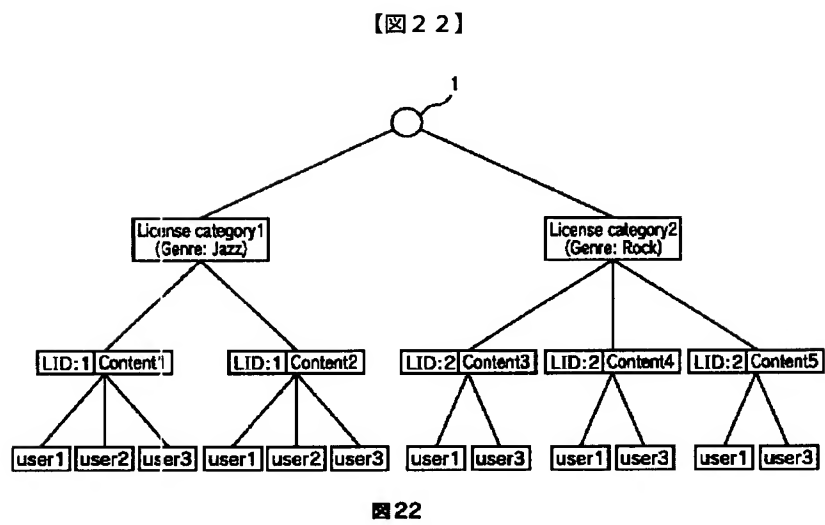
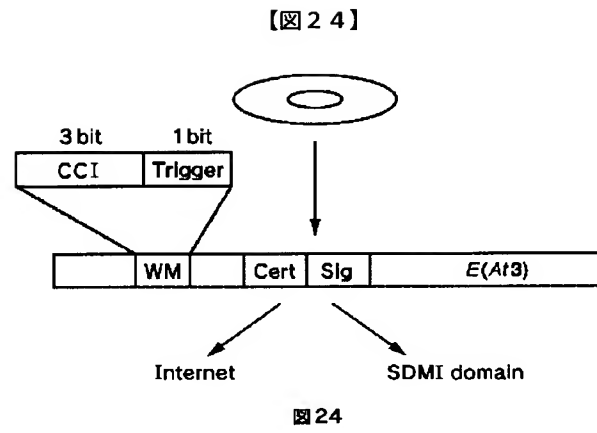
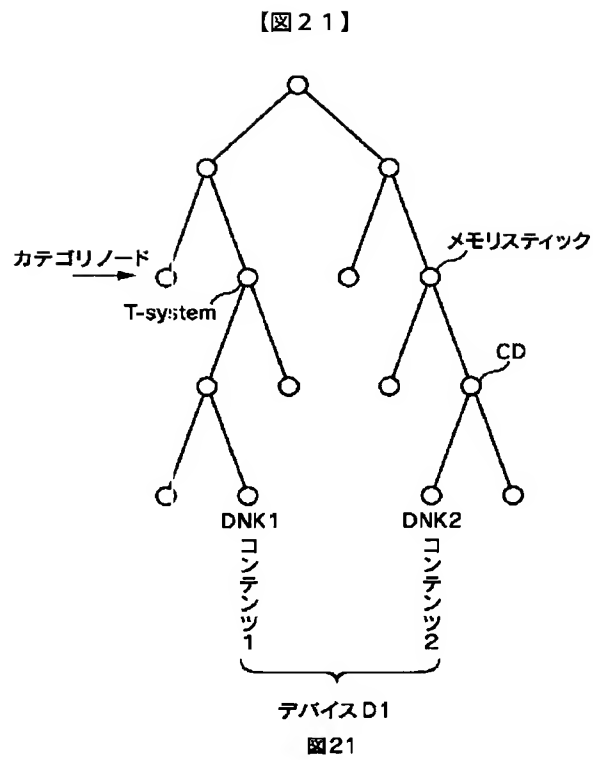


図42



【図26】

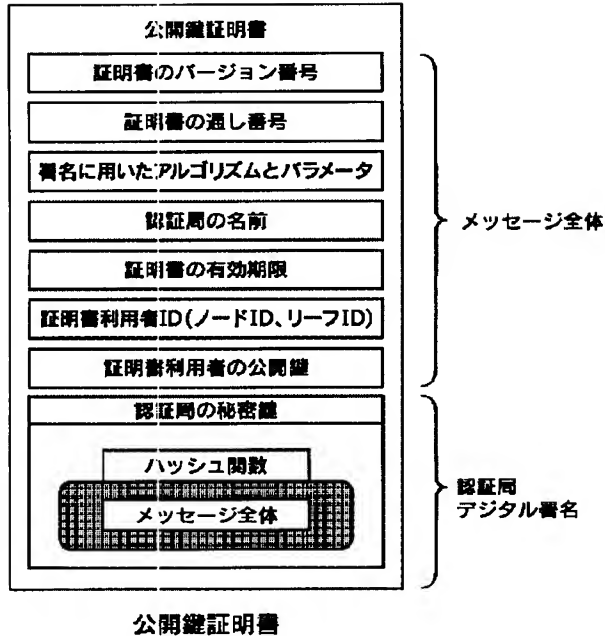
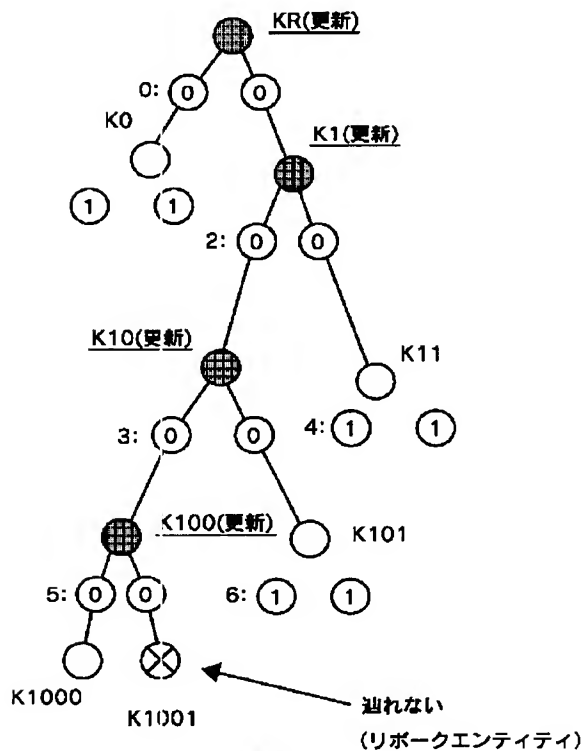


図26

【図29】



【図27】

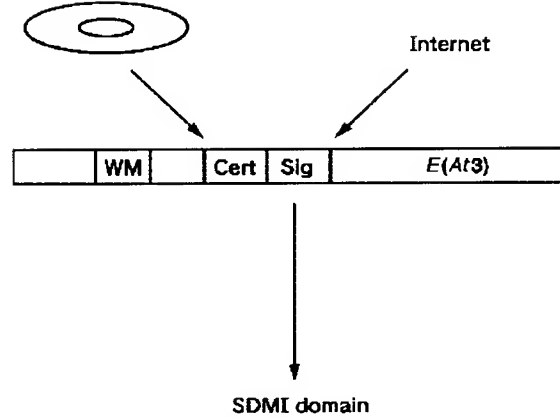
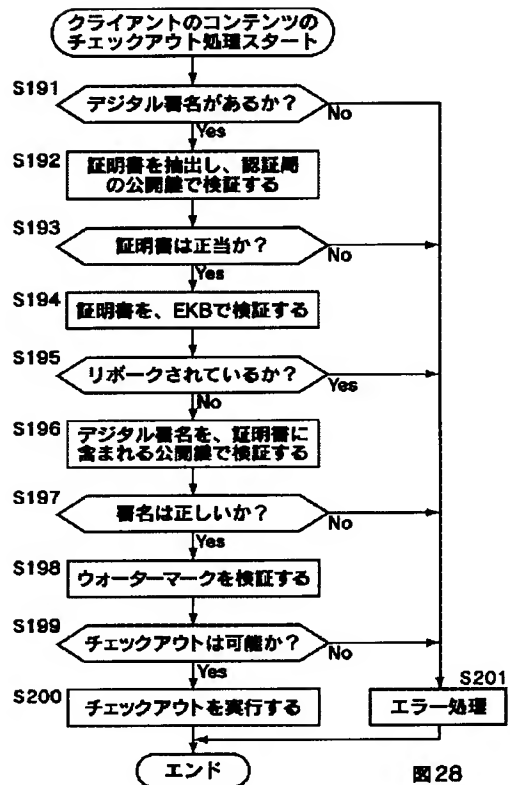


図27

【図28】



【図30】

有効化キープブロック(EKB:Enabling Key Block)の
データ部およびタグ

データ (暗号化キー)	Enc(K0, K(t)R), Enc(K(t)1, K(t)R) Enc(K(t)10, K(t)1), Enc(K11, K(t)1) Enc(K(t)100, K(t)10), Enc(K101, K(t)10) Enc(K1000, K(t)100)
タグ	0: {0, 0}, 1: {1, 1}, 2: {0, 0}, 3: {0, 0} 4: {1, 1}, 5: {0, 1}, 6: {1, 1}

{Lタグ, Rタグ}
左(L)右(R)それぞれの方向に
データがあれば0、なければ1

図30

【図32】

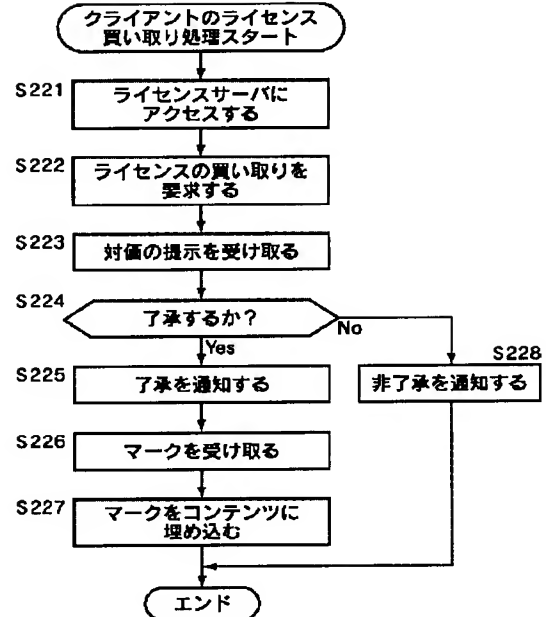


図32

【図41】

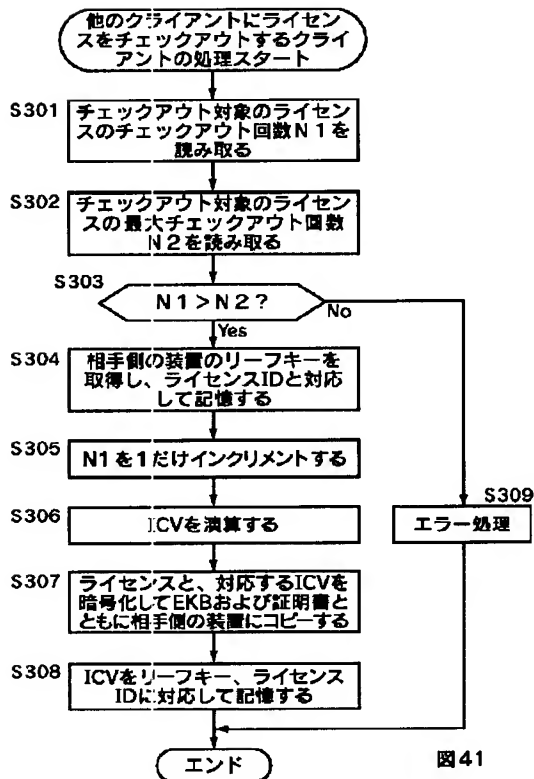


図41

【図43】

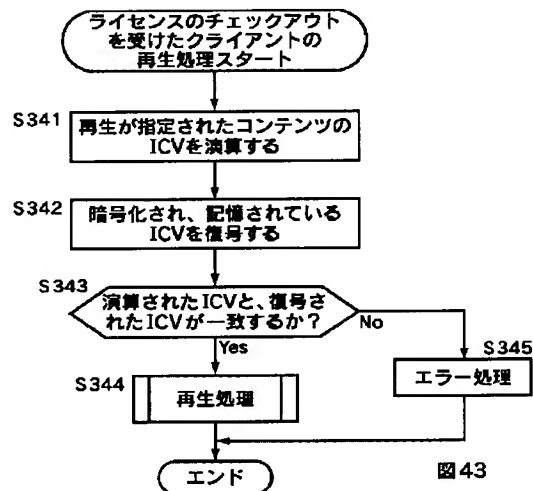


図43

【図44】

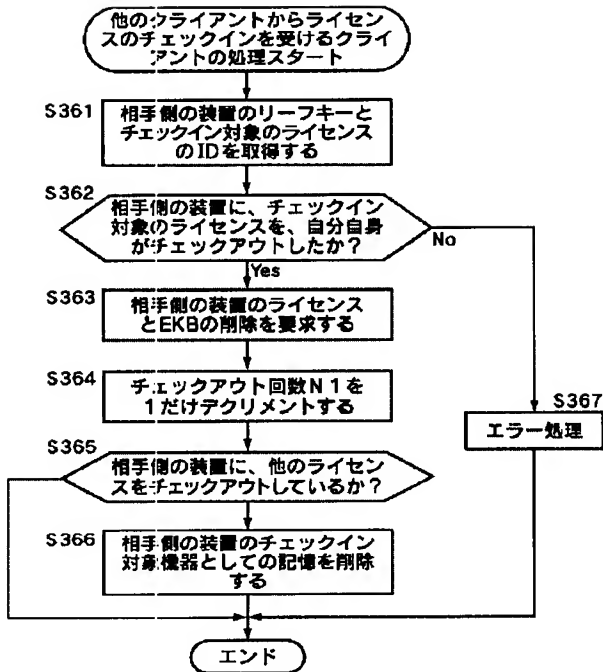


図44

【図45】

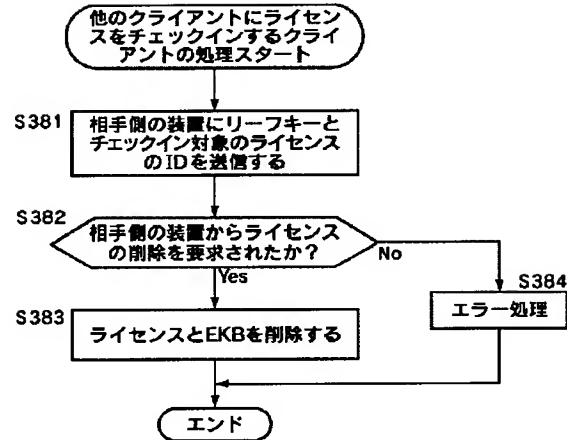


図45

【図46】

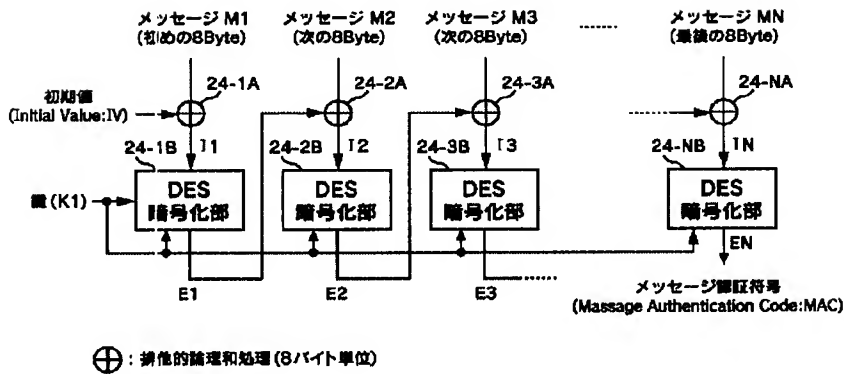


図46

【図47】

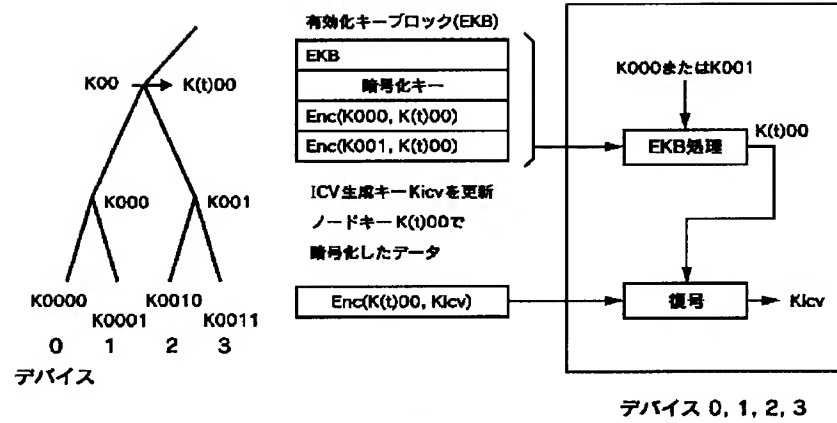


図47

【図48】

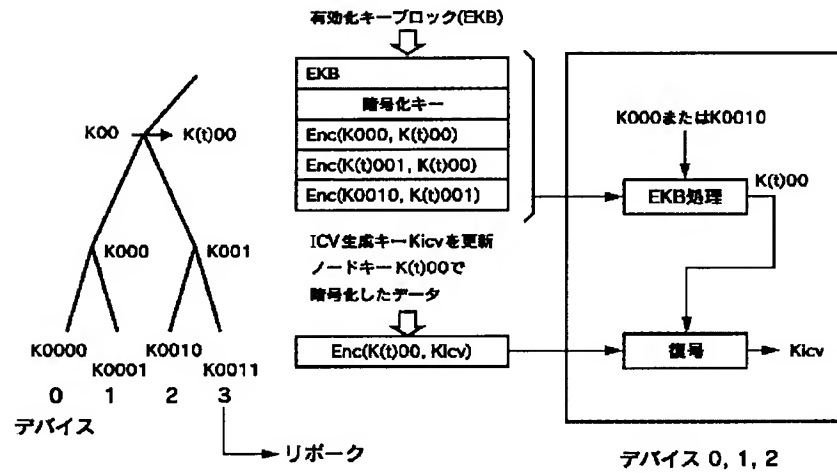


図48

【図50】

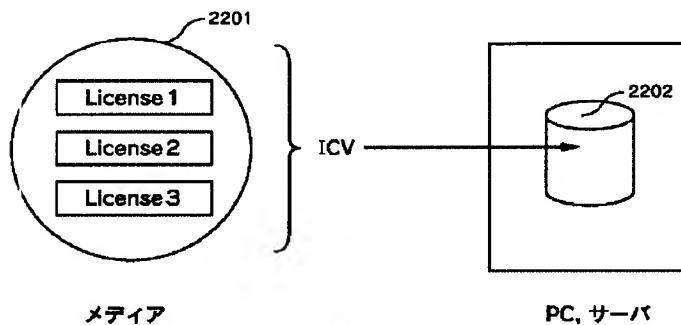


図50

【図49】

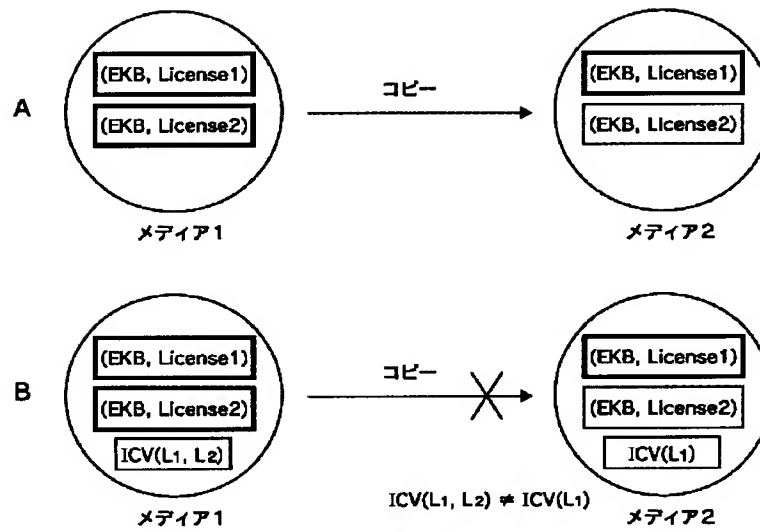


図49

フロントページの続き

(72) 発明者 黒田 壽祐
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72) 発明者 石黒 隆二
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

Fターム(参考) 5J104 AA12 MA05 PA07 PA10